LEGISLATIVE LIBRARY OF BRITISH COLUMBIA
3 3298 00338 7371

# OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER

*for*

*British Columbia*

## 2006–2007 ANNUAL REPORT

DOC
BC
I4606
B
2006/07
c.3

LEGISLATIVE LIBRARY
VICTORIA, B.C. V8V 1X4
AUG 0 1 2007

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
*for*
*British Columbia*

# 2006-2007 ANNUAL REPORT

**Library and Archives Canada Cataloguing in Publication Data**

British Columbia. Office of the Information and Privacy Commissioner.
Annual report
(CD-ROM)
Annual report [electronic resource]. –2005/2006–

Annual
CD-ROM format.
Issued also in printed form on demand.
Report year ends Mar. 31.
ISSN 1911-0278 = Annual report (British Columbia. Office of the Information & Privacy Commissioner. CD-ROM)

1. British Columbia. Office of the Information and Privacy Commissioner – Periodicals. 2. British Columbia. Freedom of information and Protection of Privacy Act. 3. Privacy, Right of – British Columbia – Periodicals. 4. Government information – British Columbia – Periodicals. 5. Public records – British Columbia – Periodicals. I. British Columbia. Office of the Information and Privacy Commissioner. II. Title.

KEB505.62 342.711'062 C2006-960094-5
KF5753.15B74

2007-05493/

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

July 26, 2007

Bill Barisoff MLA
Speaker
Legislative Assembly of British Columbia
Victoria, BC V8V 1X4

Dear Speaker:

According to s. 51 of the *Freedom of Information and Protection of Privacy Act* and s. 44 of the *Personal Information Protection Act*, I have the honour to present the Office's thirteenth Annual Report to the Legislative Assembly.

This report covers the period from April 1, 2006 to March 31, 2007.

Yours sincerely,

David Loukidelis
Information and Privacy Commissioner
for British Columbia

Mail: PO Box 9038, Stn Prov Govt, Victoria BC V8W 9A4
Location: 3rd Floor, 756 Fort Street, Victoria BC
T: 250 387 5629 F: 250 387 1696
Toll free through Enquiry BC 800 663 7867 or 604 660 2421 (Vancouver)
W: www.oipc.bc.ca

# TABLE OF CONTENTS

1 COMMISSIONER'S MESSAGE 1

1.1 FIPPA Reforms Urgently Needed ..... 1
1.2 PIPA Works Well ..... 2
1.3 Procedural and Organizational Changes Will Improve OIPC Efficiency ..... 2
1.4 Security Measures Should Not Sacrifice Privacy Rights ..... 3
1.5 Data Sharing Initiatives Must Build In Privacy Protection at the Outset ..... 3
1.6 A Citizen Registry Requires Careful Scrutiny ..... 4

2 THE YEAR IN REVIEW: STATISTICAL HIGHLIGHTS AND NOTEWORTHY INITIATIVES 5

2.1 Trends in Request for Review and Complaint Numbers ..... 5
2.2 Improvements to Procedural Efficiencies ..... 6
2.3 Privacy Breach Reporting Tools ..... 7
2.4 Policy Consultation and Legislative Reviews ..... 8
2.5 Tables ..... 10

3 CASE SUMMARIES: FIPPA MEDIATIONS, ORDERS AND SUPREME COURT ADJUDICATION 16

3.1 FIPPA Requests for Review ..... 16
3.2 FIPPA Access to Information Complaints ..... 25
3.3 FIPPA Privacy Complaints ..... 30
3.4 FIPPA Orders ..... 31
3.5 Supreme Court Review of OIPC's Openness ..... 35

4 CASE SUMMARIES: PIPA MEDIATIONS AND ORDERS 36

4.1 PIPA Requests for Review ..... 36
4.2 PIPA Complaints ..... 39
4.3 PIPA Orders ..... 46

ORGANIZATION CHART 49

FINANCIAL REPORTING 49

# 1 COMMISSIONER'S MESSAGE

## 1.1 FIPPA Reforms Urgently Needed

Another year has slipped away since unanimous Legislative Assembly review committee recommendations were made to improve the *Freedom of Information and Protection of Privacy Act* (FIPPA). The government says it has implemented some changes by policy, and a minor housekeeping amendment has been enacted, but the vitally important work of the committee sits on the shelf gathering dust. At year's end a Bill was tabled with a number of important amendments that flowed from the committee's work, but it sits there still. It seems House time ran out – I certainly hope the Bill's fate was not sealed by the hostile reaction it received from advocates of open government.

I share with the advocates of open government their biggest concern with Bill 25 – it did not restore the intended scope and meaning of the FIPPA provision that protects advice or recommendations to a public body. I have said publicly many, many times that a 2002 decision of our Court of Appeal gave the advice or recommendations exception to the public's right of access too broad an interpretation. The court's broad interpretation of advice or recommendations represents the greatest step backward in the public's right to know what is going on in government. The Legislative Assembly review committee certainly agreed and recommended specific amendments to restore openness and accountability. Courts elsewhere in Canada, notably the Ontario Court of Appeal, have rejected our appeal court's interpretation, so the government's claim that the court agrees with the government is hardly forceful.

The bottom line is that the bureaucracy is perfectly content with the Court of Appeal's crabbed view of public access to information rights under FIPPA. This is unfortunate, since it unnecessarily and inappropriately empowers more information to be hidden from the public than before. As the government increasingly removes itself from the business of providing services, focusing instead on setting policy directions, the diminishment of the public's right to access policy advice renders the government increasingly unaccountable. The Premier and Cabinet have an excellent chance here to show leadership by restoring democratic openness and accountability. In this instance, the dialogue between the courts and the Legislature should end with the Legislature asserting its supremacy and reaffirming its commitment to transparency.

## 1.2 PIPA Works Well

While we continue to wait for FIPPA reforms, the first statutory review of the *Personal Information Protection Act* (PIPA) started last year. An all-party committee has been struck and it will make recommendations on PIPA in the coming year. We will make a submission to the committee, but I can say now that our experience with PIPA over the last three years is that it is working well. Its drafting can be improved in many areas, but its design and overall thrust are balanced and effective. This is reflected I believe by the fact that the Parliamentary review of PIPA's federal cousin, the *Personal Information Protection and Electronic Documents Act*, recommended that the law be more like PIPA in a number critical areas. Still, the legislative review of PIPA offers a welcome opportunity to improve an already good piece of legislation and we will do whatever we can to help the committee do its work.

We have been very active this year in publishing resources to support private sector organizations in complying with PIPA and to help members of the public assert their privacy rights. The rise in reported privacy breaches continues and the risk of real harm ensuing – particularly fraud or identity theft – prompted us to partner with our Ontario colleagues to produce a number of related tools. These are designed to help organizations reduce the risk of data spills of all kinds and assist them in responding effectively when spills occur. Because of the sensitivity of health information, we also co-produced with the BC Medical Association and College of Physicians and Surgeons a key steps document for physicians.

As this report shows, the number of PIPA complaints was noticeably down this year, we hope because organizations continue to improve their compliance efforts. We will watch developments, of course, and in the meantime continue to investigate complaints and resolve them as effectively as we can.

While complaints were down, I had occasion to decide a number of matters under PIPA this year. One decision required me to interpret the employment privacy aspects of PIPA, another engaged analysis of work product information concepts under PIPA and others had to do with solicitor-client privilege protections under the law. Other hearings have been held and formal decisions are on the way.

## 1.3 Procedural and Organizational Changes Will Improve OIPC Efficiency

On the public sector side, access to information appeals under FIPPA continued their upward trend, moving up by 6%, while public sector privacy complaints stayed stable. My impression is that the scope and complexity of appeals that made it to the formal hearing stage increased as well, with a number of reviews and complaints concerning outsourcing arrangements proceeding to the inquiry level. Regardless of where our case numbers have headed, my office is reviewing our policies and procedures under FIPPA with a view to improving the efficiency, timeliness and quality of our work. We have among other things speeded up our handling of procedural objections, implemented

an early intervention process for simple matters and, perhaps most significantly, fast-tracked deemed refusals, which involve failures by public bodies to disclose records on time.

We also instituted organizational changes, most significantly by creating new managerial positions. Our two Managers of Investigations and Mediation oversee the work of our Portfolio Officers and Intake Officers in order to support their work while ensuring quality control. Although technically effective only at the start of 2007-2008, I will note that we have also filled two new Portfolio Officer positions using funds approved by the Legislative Assembly committee responsible for our budget. We hope to make these positions permanent as they are critical to our ability to respond in a timely and effective fashion to complaints, appeals and other demands for our services.

## 1.4 Security Measures Should Not Sacrifice Privacy Rights

I yet again express my concern about privacy and the push for more state intrusion in the name of national security, fighting terrorism and law enforcement. Many of us mistakenly undervalue our privacy. The importance of privacy is illustrated, however, by the impact of privacy breaches. The Arar commission illustrates this. Maher Arar was deported, incarcerated and tortured because of inaccurate personal information that was improperly shared and used. Closer to home, your inclusion on a terrorist watch list or no-fly list will inconvenience you, embarrass you and can cost you your job or worse.

Against these real costs of privacy violations, we see governments pressing for more access to personal information and more freedom to use it. If you have nothing to hide, why not let government know everything about you? Benjamin Franklin famously said those who would sacrifice freedom for temporary security deserve neither. It remains government's burden in our liberal democracy to justify its intrusion on our liberty. Unless the state can show, based on real evidence and not mere politics or cynical expedience, that it has a compelling need to limit our liberty, our business is not the government's business. We need to remember this in these fear-driven times, where the risk and contingency that are part of life are magnified and used to justify greater control over us. Of course we need to fight terrorism and of course we need to protect citizens from harm. But we must not hand the state a blank cheque to do whatever it asserts is warranted

## 1.5 Data Sharing Initiatives Must Build In Privacy Protection at the Outset

Outside the law and order sphere, governments everywhere, including in British Columbia, are moving to integrate information systems as they seek to revamp how they deliver services. More and more I am hearing calls for government to 'break down the data silos', to provide citizen-centred services using personal information from disparate sources. No one disputes that efficient and effective service delivery warrants appropriate sharing of personal information.

In British Columbia, FIPPA already gives public servants considerable latitude in sharing personal information to deliver common or integrated programs or services.

But in breaking down the silos, in liberating data, governments must take care to design privacy into systems from the get-go. Privacy is not an after-market option that can be clamped onto the box once it is running. Data sharing programs must be built within the framework of the existing privacy laws. The privacy rights of BC citizens must not be weakened merely to facilitate greater data sharing amongst government officials.

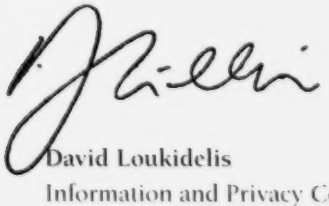
The provincial government is designing a secure information access network that will enable the sharing of personal information across government programs and agencies. Government is researching and formulating privacy and security policy choices around access to this system. We have been briefed on progress to date and will keep a close eye on what is happening. More directly, because it is imperative that privacy be designed in and protected, we are working on data sharing principles that we will use to assess government's policy choices. That guidance will be published as soon as possible in 2007-2008 and we will use it to, among other things, assess the Ministry of Health's electronic health records initiative.

## 1.6 A Citizen Registry Requires Careful Scrutiny

A related issue is whether British Columbia should have a citizen registry. We commented adversely this year on a number of legislative and program proposals for use of existing registry-like databases, notably the Medical Services Plan registry of British Columbia residents registered with MSP. Government ministries have sought to use MSP name and address data to locate individuals for a variety of reasons, but the unifying feature of their efforts is that they would like to use MSP as a citizen registry for many purposes.

I stiffly resisted these attempts to use personal information in MSP, which after all is collected and compiled for health care administration purposes only and which has legislative protection ensuring that limited use. Rather than continuing with *ad hoc* ministry-by-ministry attempts to gain access to MSP, the government should examine whether a true, purpose-built citizen registry is acceptable.

That decision is certainly not mine to make, but it is a critically important choice. It is not an esoteric or technical matter – among other things, population registries are the backbone of identity cards and identification systems. Such a decision should be made only after careful scrutiny and meaningful public consultation.



**David Loukidelis**
Information and Privacy Commissioner for British Columbia
July 2007

# 2 THE YEAR IN REVIEW: STATISTICAL HIGHLIGHTS AND NOTEWORTHY INITIATIVES

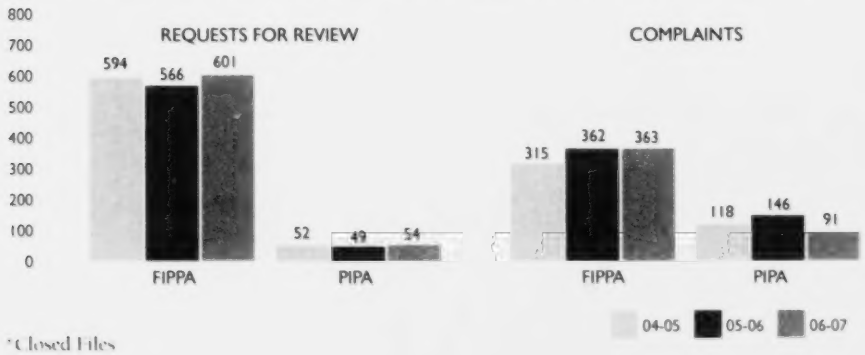
The tables in this part of the report provide a numerical snapshot of the work of the Office of the Information and Privacy Commissioner in 2006-07 (our fiscal year runs from April 1 to March 31). Table 1 provides an overview of all of our activities during the year and comparable figures from the previous two years. Tables 2 through 6 provide details of the types of requests for review and complaints we dealt with under the *Freedom of Information and Protection of Privacy Act* (FIPPA) as well as a list of the public bodies that most frequently were the subjects of requests for review and complaints. To round out the statistical summary, Tables 7 and 8 detail the types of requests for review and complaints we handled under the *Personal Information Protection Act* (PIPA).

## 2.1 Trends in Request for Review and Complaint Numbers

Dealing with requests for review and complaints about non-compliance with FIPPA or PIPA is the bread and butter of our work, as it is through these mechanisms that ordinary citizens exercise their rights under the two laws that we oversee. Requests for review involve our review of decisions not to release information or, on occasion, not to correct personal information. Complaints can be about a variety of concerns, ranging from unauthorized collection, use and disclosure of personal information under FIPPA or PIPA to inadequate searches for records requested under FIPPA.

In 2006-07, we closed 655 request-for-review files (601 under FIPPA and 54 under PIPA) and 454 complaint files (363 under FIPPA and 91 under PIPA).

FIGURE 1 FIPPA AND PIPA REQUESTS FOR REVIEW AND COMPLAINTS 2004-07*




*Closed Files

As illustrated by Figure 1, the number of requests for review closed under FIPPA and PIPA and of complaints closed under FIPPA has increased over the past three years. There has, however, been a noticeable dip in the number of PIPA complaints, from 146 to 91, between 2005-06 and 2006-07. We believe this reflects the concerted effort that organizations subject to PIPA, such as provincially regulated companies and non-profit societies, have been making to get up to speed with their statutory obligations to deal appropriately with customers' personal information. As a result of the publicity surrounding the coming into force of PIPA in January 2004, and its federal counterpart the *Personal Information Protection and Electronic Documents Act* (PIPEDA), consumers were quick to become aware of and begin to exercise their new rights under the legislation, and we received a flurry of requests for review and complaints from the outset.

Not surprisingly, it took some time for organizations to develop the privacy policies and practices needed to ensure effective compliance with PIPA. To do so was especially challenging for small businesses with few resources to meet their new obligations. During the past three years, we have provided considerable guidance not only through direct communication with individual businesses and associations but also through a series of guidelines published on our website. The reduction in PIPA complaints suggests these efforts are paying off.

We are continuing to build on this work by co-hosting our second annual PIPA Conference, "Private Sector Privacy in a Changing World", in Vancouver, September 20 and 21, 2007. The OIPC continues, of course, to investigate complaints and take formal action where appropriate, but at the same time we continue to provide compliance support for organizations, consumers and employees.

## 2.2 Improvements to Procedural Efficiencies

With 21 staff, we manage to run a lean and efficient operation, but there is always room for improvement, and we still face challenges resulting from earlier years' cuts to our budget for public sector oversight duties. As Table 1 indicates, the total number of files we handled during this fiscal year, while somewhat lower than last year, still represents an increase of one-third over the 2004-05 total. To improve our ability to manage a large number and wide diversity of files while increasing the speed of our response to requests for review and complaints, in 2006-07 we took several steps to maximize efficiency. These included implementing:

- An early intervention process for quick resolution of simple requests for review and complaints. Under this process, files that have been opened by our Intake team are channelled to a designated early intervention Portfolio Officer, who identifies issues capable of quick resolution and takes the necessary steps, including mediation where necessary, to bring the file to a rapid conclusion. More complex files are then assigned to another Portfolio Officer for further investigation and mediation.

- An expedited deemed refusal process for complaints about public bodies' failure to respond in time to access to information requests. Complaints that public bodies have exceeded the 30-day timeline prescribed by section 7 of FIPPA, where the permission of our office for a time extension has not been sought and obtained under section 10, no longer take their place in the mediation queue but instead are routed immediately to a designated Portfolio Officer, who contacts the public body, determines the reason for the delay and arrives at a fixed date for response by the public body to the access request. We then issue to all parties a consent order specifying the agreed-upon date. This consent order has the same force as an order issued by the Commissioner. If the date is missed, the matter may proceed to an expedited inquiry.
- Fast-tracking of procedural objections at inquiry. Objections by parties on matters such as whether material is properly submitted by a public body *in camera* (in secret) or the relevance of a party's submission are now dealt with at the time they occur instead of during the hearing, thus ensuring that procedural issues are dealt with right away and do not cause delay down the road.
- Restructuring of management responsibilities. To improve quality control and increase the effectiveness of our oversight responsibilities, we appointed two Managers of Investigation and Mediation with separate lead responsibilities for each statute. Their primary role is to support the work of Portfolio Officers and Intake Officers, provide expert guidance on complex investigations and engage in policy consultations on current issues.
- Appointment of a half-time adjudicator. The creation of this position, complementing the roles of the Senior Adjudicator and the Commissioner in writing orders, is intended to enable us to significantly reduce our backlog of inquiry decisions.
- Appointment of additional Portfolio Officers. The addition of three new Portfolio Officers with diverse backgrounds has further helped reduce the backlog of request for review and complaint files so that we are able to respond in a timely manner to new requests and complaints. Two of these positions are one-year appointments only, as discussed in the Commissioner's message in this report.

## 2.3 Privacy Breach Reporting Tools

As Table 1 indicates, the number of times we have been notified of privacy breaches has risen dramatically in the past three years. Public sensitivity about inappropriate access to personal information has never been higher and there has been much publicity recently about breaches of privacy resulting from inappropriate disclosure of information, whether through deliberate actions, careless disposal of documents or other circumstances. FIPPA (section 30) and PIPA (section 34) require public bodies

and organizations to make reasonable security arrangements to guard against such risks as unauthorized access, collection, use, disclosure or disposal of personal information in their custody or control, but inevitably breaches occur. Case Summary 23 in Part 3 of this report and Case Summaries 37 and 38 in Part 4 illustrate privacy breaches brought to our attention.

Because of our concern about the rise in the number of reported breaches, and about the consequences for affected individuals, during the past year we published on our website three documents that provide guidance on appropriate steps to be taken in the event of a breach:

- "Key Steps in Responding to Privacy Breaches" describes how to identify when a breach has occurred and emphasizes the importance of responding promptly by containing the breach, evaluating the risks associated with the breach, deciding whether and how to notify affected individuals and determining the steps needed to prevent future breaches.[1]
- "Privacy Breach Reporting Form" is for use by public bodies and organizations in reporting a privacy breach to our office.[2]
- "Breach Notification Assessment Tool" helps public bodies and organizations decide whether, when and how to notify affected individuals of a breach.[3]

We continue, as well, to provide guidance on recommended security measures to ensure compliance with FIPPA and PIPA privacy protection requirements. For example, in June 2006, in co-operation with the College of Physicians and Surgeons and the British Columbia Medical Association, we posted on our website "Physicians and Security of Personal Information"[4] and "Key Steps for Physicians in Responding to Security Breaches".[5]

## 2.4 Policy Consultation and Legislative Reviews

### POLICY CONSULTATION

Under the general powers provided to the Commissioner under section 42 of FIPPA and section 36 of PIPA, we actively consult not only with public bodies and organizations but also with our counterparts in other jurisdictions on policy matters of current significance. In 2006-07, we engaged in policy consultations on a large number of initiatives, including these representative examples:

- Statistics Canada as part of the 2006 Census Consultation;
- the Ministry of Health on the Chronic Disease Management (CDM) Toolkit;
- the federal Ministers of Industry and Canadian Heritage on copyright reform, digital rights management and privacy protection;
- the Ministry of Health on the privacy strategy related to the Electronic Health Record (EHR);
- the Insurance Corporation of British Columbia and Ministry of Solicitor General on the Washington-BC secure driver's licence initiative for expedited border crossing into the US;

[1] http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf
[2] http://www.oipc.bc.ca/forms/Privacy_Breach_Form_(Dec_2006).pdf
[3] http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf
[4] http://www.oipc.bc.ca/pdfs/private/PhysicianSecurityofpersonalinformation.pdf
[5] http://www.oipc.bc.ca/pdfs/private/PhysicianKeyStepsPrivacyBreach.pdf

- the Provincial Health Services Authority regarding the Provincial Surgical Services Project;
- the federal Department of Justice on identity theft;
- the Victoria Police Department on covert video surveillance technology;
- the Chief Information Officer on the proposed provincial government Secure Information Access Network (SIAN);
- the newly established Office of the Representative for Children and Youth on access and privacy issues; and
- the Ministry of Education on the proposed teacher registry and on Ministry collection, use and disclosure of personal information in association with students' personal education numbers.

In August 2006, following extensive consultation with municipalities, the Commissioner released a discussion paper entitled "Local Governments and the Growth of Surveillance", which addresses the recent practice among some municipalities of passing bylaws compelling certain types of businesses to collect customers' personal information and make it available to the police routinely and without suspicion, much less cause. The discussion paper, which is posted on our website,[6] concludes that the risks to innocent citizens' privacy posed by such surveillance bylaws outweigh possible public benefits and that court-ordered warrants, consistent with Canadian law and practice, remain the preferred approach.

On the private sector side, in addition to consulting with the medical community in developing the security guidelines described above, we worked with the Retail Council of Canada and the Alberta OIPC to publish "Privacy Proofing Your Retail Business"[7] for publication in ***Canadian Retailer*** magazine.

## LEGISLATIVE REVIEWS

As a matter of course, we review every Bill presented to the British Columbia Legislative Assembly for potential access and privacy implications. We also comment on proposed legislative initiatives when public bodies invite us to do so. We strongly encourage public bodies to consult with us before introduction of a Bill so we can identify access and privacy issues and suggest appropriate solutions to potential problems.

In addition to making presentations to the all-party Special Committee to Review the *Personal Information Protection Act*, the Commissioner appeared before the House of Commons Standing Committee on Access to Information, Privacy and Ethics, during its statutory review of PIPEDA, to provide insights about the effectiveness of PIPA (which is substantially similar to PIPEDA). In its fourth report to Parliament in May 2007, the committee spoke highly of BC's PIPA and several of the committee's recommendations were that PIPA provisions would provide a useful model for consideration during the drafting of amendments to PIPEDA.

[6] http://www.oipc.bc.ca/publications/SurveillanceBylawDiscussionPaper.pdf
[7] http://www.oipc.bc.ca/pdfs/private/Privacy_Proof_Retail_Bus(OIPC).pdf

TABLE 1 FIPPA AND PIPA FILES RECEIVED AND CLOSED, 1 APRIL 2006 – 31 MARCH 2007

| | | DISPOSITION | | |
|---|---|---|---|---|
| **FILE TYPE** | RECEIVED 06/07 | CLOSED 06/07 | CLOSED 05/06 | CLOSED 04/05 |
| ***Information requested/received*** | | | | |
| Requests for information | 2783 | 2781 | 3694 | 1761 |
| Read and file | 99 | 98 | -* | 130 |
| Media queries | 39 | 37 | 68 | 97 |
| Freedom of information requests for OIPC records | 4 | 4 | 9 | 23 |
| ***Requests for review*** | | | | |
| Requests for review of decisions to withhold information | 598 | 655 | 615 | 644 |
| Applications to disregard requests as frivolous or vexatious | 6 | 5 | 5 | 4 |
| ***Complaints*** | | | | |
| Complaints about non-compliance with FIPPA or PIPA | 455 | 454 | 508 | 433 |
| ***Reviews/investigations declined*** | | | | |
| Non-jurisdictional | 29 | 27 | 26 | 22 |
| No reviewable issue | 104 | 103 | 23 | 30 |
| ***Requests for time extension*** | | | | |
| By public bodies/organizations for time extension | 242 | 244 | 79 | 115** |
| By applicants for time extension to request a review | 17 | 18 | 27 | - |
| ***Reconsideration of decisions*** | | | | |
| Internal reconsideration of OIPC decisions | 5 | 4 | 6 | 11 |
| Adjudication | 1 | 1 | 0 | 1 |
| ***Files initiated by public bodies/organizations*** | | | | |
| Privacy impact assessments | 9 | 9 | 2 | 7 |
| Public interest notification | 7 | 7 | 10 | 25 |
| Notification of privacy breaches | 86 | 72 | 23 | 3 |
| ***OIPC-initiated files*** | | | | |
| Systemic investigations | 10 | 10 | 14 | 6 |
| Special projects | 28 | 20 | 29 | 27 |
| Reviews of proposed legislation | 52 | 55 | 37 | 75 |
| ***Policy or issue consultations*** | 133 | 112 | 188 | 127 |
| ***Public education/outreach*** | | | | |
| Speaking engagements by OIPC staff | 57 | 50 | 68 | 40 |
| Conference attendance | 13 | 10 | 20 | |
| Meetings with public bodies/organizations | 34 | 30 | 43 | 31 |
| Site visits by Commissioner to public bodies/organizations | 3 | 3 | 6 | - |
| ***Other*** | 14 | 16 | 8 | 1 |
| **Totals** | **4828** | **4825** | **5504** | **3613** |

* Included in the requests for information total in 2005-06.

** This figure includes requests both by applicants and by public bodies/organizations.

## TABLE 1 EXPLANATORY NOTES

*Information requested/received*
Members of the public and organizations contact us regularly with questions about FIPPA and PIPA requirements. "Read and file" refers primarily to correspondence copied to the OIPC.

*Requests for review*
Our largest activity each year involves processing requests for review of decisions by public bodies and organizations to withhold information. The 655 requests for review we completed this year included 601 under FIPPA (Table 2) and 54 under PIPA (Table 8). On rare occasions, public bodies apply to have such requests dismissed as frivolous or vexatious under section 43 of FIPPA; section 37 of PIPA authorizes private organizations to make similar applications.

*Complaints*
The 454 complaint files closed this year included 363 under FIPPA, of which 241 related to access to information and 122 related to protection of privacy (Tables 4 and 5). The 91 PIPA complaints (Table 7) represented a significant drop from the previous year. (FIPPA complaints and requests for review under both Acts increased in number.)

*Reviews/investigations declined*
We may decline to investigate a complaint for a number of reasons (e.g., the complaint is frivolous or vexatious, no remedy is available or we do not have jurisdiction to examine the matter). When we decline to investigate a complaint or conduct a review because we lack jurisdiction, we try to direct the complainant or applicant to the appropriate body with the authority to address the concern (e.g., the federal Privacy Commissioner for private sector complaints against organizations that are not provincially regulated or the RCMP for complaints against that organization; in addition, we receive complaints against bodies such as BC Ferries that government has specifically excluded from the application of FIPPA).

*Requests for time extension*
Section 10 of FIPPA and section 31 of PIPA authorize public bodies and organizations respectively to ask our office for a time extension to respond to an access request under certain circumstances. Section 53 of FIPPA and section 47 of PIPA authorize applicants to ask us for permission to request a review more than 30 days after notification of the public body's or organization's decision.

*Reconsideration of decisions*
If a complainant presents new information after we have completed an investigation, we may reconsider our findings in light of that information. "Adjudication" in this instance refers to a review by a judge of a complaint about a decision, act or failure to act by the Commissioner as head of a public body. (See summary at section 3.5 of this report.)

*Files initiated by public bodies or organizations*
Public bodies and private organizations frequently ask us for advice on privacy/access implications of proposed policies or current issues or may ask us to review privacy impact assessments they have prepared for proposed policies or programs. Section 25 of FIPPA requires public bodies to disclose certain information in the public interest and to first notify us.

*OIPC-initiated files*

Investigations of individual complaints may trigger concerns about systemic issues in the operations of a public body, leading to a broader investigation. Special projects include initiatives such as policy research and preparation of guidelines for FIPPA and PIPA compliance published on our website. In addition to reviewing all bills presented to the Legislative Assembly for FIPPA or PIPA implications, we provide advice on the drafting of bills at the invitation of public bodies.

*Public education and outreach*

Our public education activities include frequent presentations to community groups, business organizations and conferences on current issues as well as information on complying with PIPA and FIPPA. We also meet individually with public bodies and organizations as the need arises and the Commissioner conducts site visits to assess and provide advice on compliance with the laws we administer.

TABLE 2 DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY TYPE

| | DISPOSITION | | | | | | |
|---|---|---|---|---|---|---|---|
| **TYPE** | MEDIATED | NO REVIEWABLE ISSUE | REFERRED TO PUBLIC BODY | WITHDRAWN | OTHER DECISION BY COMMISSIONER | NOTICE OF INQUIRY ISSUED | TOTAL |
| Deemed refusal | 109 | 12 | 2 | 6 | 0 | 3 | 132 |
| Deny access | 47 | 3 | 1 | 9 | 1 | 10 | 71 |
| Notwithstanding | 3 | 1 | 0 | 0 | 0 | 0 | 4 |
| Partial access | 310 | 10 | 1 | 27 | 1 | 16 | 365 |
| Refusal to confirm or deny | 1 | 0 | 0 | 1 | 0 | 0 | 2 |
| Scope | 5 | 3 | 0 | 0 | 0 | 1 | 9 |
| Third party | 10 | 0 | 0 | 4 | 0 | 4 | 18 |
| **Total** | **485** | **29** | **4** | **47** | **2** | **34** | **601** |

TABLE 2 DEFINITIONS

Deemed refusal: Failure to respond within required timelines (s. 7)
Deny access: All information withheld from applicant (ss. 12-22)
Notwithstanding: Conflict between FIPPA and other legislation (s. 79)
Partial access: Some information withheld from applicant (ss. 12-22)
Refusal to confirm or deny: Refusal by public body to confirm or deny the existence of responsive records (s. 8)
Scope: Requested records not covered by FIPPA (ss. 3-4)

TABLE 3 DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY PUBLIC BODY

| | DISPOSITION | | | | | | |
|---|---|---|---|---|---|---|---|
| PUBLIC BODY (TOP 10) | MEDIATED | NO REVIEWABLE ISSUE | REFERRED BACK TO PUBLIC BODY | WITHDRAWN | OTHER DECISION BY COMMISSIONER | NOTICE OF INQUIRY ISSUED | TOTAL |
| Insurance Corporation of BC | 164 | 2 | 1 | 10 | 0 | 1 | 178 |
| Ministry of Attorney General | 20 | 2 | 2 | 3 | 0 | 1 | 28 |
| Ministry of Public Safety and Solicitor General | 21 | 1 | 0 | 2 | 0 | 3 | 27 |
| Ministry of Children and Family Development | 21 | 3 | 0 | 1 | 0 | 0 | 25 |
| Vancouver Police Department | 14 | 2 | 0 | 5 | 0 | 1 | 22 |
| Ministry of Health | 9 | 1 | 0 | 1 | 0 | 4 | 15 |
| Ministry of Finance | 12 | 0 | 0 | 0 | 0 | 2 | 14 |
| Vancouver Island Health Authority | 11 | 2 | 0 | 0 | 0 | 0 | 13 |
| Ministry of Small Business and Revenue (now Provincial Revenue) | 7 | 1 | 0 | 2 | 0 | 2 | 12 |
| WorkSafeBC | 6 | 3 | 0 | 1 | 0 | 1 | 11 |
| Northern Health Authority | 11 | 0 | 0 | 0 | 0 | 0 | 11 |
| All other public bodies | 189 | 12 | 1 | 22 | 2 | 19 | 245 |
| **Total** | **485** | **29** | **4** | **47** | **2** | **34** | **601** |

TABLE 3 EXPLANATORY NOTES

In this as in every other year, the great majority of ICBC requests for reviewed are filed by lawyers performing due diligence on behalf of clients involved in motor vehicle accident lawsuits. As with ICBC, the number of requests for review and complaints against a public body is not necessarily indicative of non-compliance but may be a reflection of its business model or of the quantity of personal information involved in its activities.

TABLE 4 DISPOSITION OF FIPPA ACCESS COMPLAINTS, BY TYPE

| | DISPOSITION | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| TYPE | MEDIATED | NOT SUBSTANTIATED | PARTIALLY SUBSTANTIATED | SUBSTANTIATED | REFERRED BACK TO PUBLIC BODY | NO REVIEWABLE ISSUE | WITHDRAWN | DECLINED TO INVESTIGATE | NOTICE OF INQUIRY ISSUED | TOTAL |
| Adequate search | 9 | 23 | 7 | 1 | 20 | 1 | 5 | 0 | 0 | 66 |
| Duty required by Act | 52 | 20 | 5 | 8 | 22 | 8 | 9 | 3 | 2 | 129 |
| Fees | 11 | 4 | 0 | 1 | 17 | 4 | 7 | 1 | 1 | 46 |
| Time extension by PB | 8 | 8 | 0 | 3 | 0 | 1 | 3 | 0 | 0 | 23 |
| **Total** | **80** | **55** | **12** | **13** | **59** | **14** | **24** | **4** | **3** | **264** |

TABLE 4 DEFINITIONS

Adequate search: Failure to conduct adequate search for records (s. 6).
Duty required by Act: Failure to fulfil any duty required by FIPPA (other than an adequate search).
Fees: Unauthorized or excessive fees assessed by public body (s. 75).
Time extension: Unauthorized time extension taken by public body (s. 10).

TABLE 5 DISPOSITION OF FIPPA PRIVACY COMPLAINTS, BY TYPE

| | DISPOSITION | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| TYPE | MEDIATED | NOT SUBSTANTIATED | PARTIALLY SUBSTANTIATED | SUBSTANTIATED | REFERRED BACK TO PUBLIC BODY | NO REVIEWABLE ISSUE | WITHDRAWN | DECLINED TO INVESTIGATE | NOTICE OF INQUIRY ISSUED | TOTAL |
| Collection | 2 | 10 | 0 | 1 | 8 | 3 | 1 | 2 | 3 | 30 |
| Correction | 4 | 2 | 0 | 0 | 8 | 2 | 0 | 0 | 0 | 16 |
| Disclosure | 6 | 8 | 3 | 4 | 9 | 4 | 2 | 1 | 2 | 39 |
| Retention | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 |
| Use | 1 | 3 | 1 | 3 | 3 | 0 | 0 | 0 | 0 | 11 |
| **Total** | **13** | **26** | **4** | **8** | **28** | **9** | **3** | **3** | **5** | **99** |

TABLE 5 DEFINITIONS

Collection: Unauthorized collection of information (ss. 26 and 27).
Correction: Refusal to correct or annotate information in a record (s. 29).
Disclosure: Unauthorized disclosure by the public body (s. 33).
Retention: Failure to retain information for time required (s. 31).

TABLE 6 FIPPA ACCESS AND PRIVACY COMPLAINTS, BY PUBLIC BODY

| | DISPOSITION | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| PUBLIC BODY | ADEQUATE SEARCH | COLLECTION | CORRECTION | DISCLOSURE | OTHER DUTY REQUIRED BY ACT | FEES | RETENTION | TIME EXTENSION BY PUBLIC BODY | USE | TOTAL |
| Insurance Corporation of BC | 7 | 4 | 1 | 4 | 25 | 3 | 0 | 1 | 1 | 46 |
| WorkSafeBC | 3 | 3 | 3 | 7 | 4 | 1 | 1 | 0 | 0 | 22 |
| Ministry of Children and Family Development | 4 | 4 | 1 | 5 | 4 | 0 | 0 | 0 | 4 | 22 |
| Ministry of Finance | 3 | 0 | 0 | 0 | 9 | 1 | 0 | 2 | 0 | 15 |
| Ministry of Health | 1 | 2 | 1 | 2 | 2 | 4 | 0 | 0 | 2 | 14 |
| Ministry of Attorney General | 1 | 1 | 0 | 2 | 6 | 1 | 0 | 2 | 0 | 13 |
| Vancouver Island Health Authority | 2 | 2 | 1 | 0 | 6 | 0 | 0 | 1 | 0 | 12 |
| Ministry of Employment and Income Assistance | 4 | 0 | 2 | 2 | 1 | 0 | 0 | 0 | 1 | 10 |
| Ministry of Public Safety and Solicitor General | 0 | 0 | 0 | 1 | 5 | 1 | 0 | 2 | 0 | 9 |
| City of Vancouver | 2 | 0 | 0 | 1 | 3 | 2 | 0 | 1 | 0 | 9 |
| All other public bodies | 39 | 14 | 7 | 15 | 65 | 32 | 2 | 14 | 3 | 191 |
| **Total** | **66** | **30** | **16** | **39** | **130** | **45** | **3** | **23** | **11** | **363** |

TABLE 7 DISPOSITION OF PIPA COMPLAINTS, BY TYPE

| | DISPOSITION | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| TYPE | MEDIATED | NOT SUBSTANTIATED | PARTIALLY SUBSTANTIATED | SUBSTANTIATED | REFERRED BACK TO ORGANIZATION | NO REVIEWABLE ISSUE | WITHDRAWN | DECLINED TO INVESTIGATE | NOTICE OF INQUIRY ISSUED | TOTAL |
| Adequate search | 0 | 1 | 2 | 0 | 1 | 0 | 0 | 1 | 0 | 5 |
| Collection | 3 | 4 | 0 | 0 | 4 | 2 | 6 | 2 | 1 | 22 |
| Correction | 0 | 0 | 0 | 0 | 3 | 0 | 1 | 0 | 0 | 4 |
| Disclosure | 5 | 1 | 1 | 1 | 7 | 2 | 3 | 3 | 0 | 23 |
| Duty required by Act | 8 | 6 | 0 | 0 | 5 | 3 | 2 | 1 | 1 | 26 |
| Fees | 2 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 4 |
| Protection/retaliation | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Retention | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Use | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 2 | 0 | 6 |
| **Total** | **20** | **12** | **3** | **1** | **21** | **9** | **13** | **9** | **3** | **91** |

TABLE 7 DEFINITIONS

Adequate search: Failure to conduct adequate search for records (s. 28).
Collection: Inappropriate collection of information (s. 11).
Correction: Refusal to correct or annotate information in a record (s. 24).
Disclosure: Inappropriate disclosure of personal information (s. 17).
Duty required by Act: Failure to fulfil any duty required by PIPA (other than an adequate search).
Fees: Unauthorized or excessive fees assessed by organization (s. 32).
Protection/retaliation: Reprisal against employee (s. 54).
Retention: Failure to retain personal information for time required (s. 35).
Use: Inappropriate use of personal information (s. 14).

TABLE 8 DISPOSITION OF PIPA REQUESTS FOR REVIEW, BY TYPE

| | DISPOSITION | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| TYPE | MEDIATED | NO REVIEWABLE ISSUE | NON JURISDICTIONAL | REFERRED BACK TO ORGANIZATION | WITHDRAWN | DECLINED TO INVESTIGATE | NOTICE OF INQUIRY ISSUED | TOTAL |
| Deemed refusal | 31 | 5 | 1 | 1 | 1 | 0 | 1 | 40 |
| Deny access | 5 | 3 | 0 | 0 | 0 | 0 | 0 | 8 |
| Partial access | 3 | 1 | 0 | 0 | 1 | 1 | 0 | 6 |
| **Total** | **39** | **9** | **1** | **1** | **2** | **1** | **1** | **54** |

TABLE 8 DEFINITIONS

Deemed refusal: Failure to respond to request for personal information (s. 28).
Deny access: All personal information withheld from applicant (s. 23).
Partial access: Some personal information withheld from applicant (s. 23).

# 3 CASE SUMMARIES: FIPPA MEDIATIONS, ORDERS AND SUPREME COURT ADJUDICATION

The following summaries are grouped according to the sections of FIPPA to which they most closely relate. For a more detailed analysis of how we interpret FIPPA when dealing with requests for review and complaints, a sectional index on our website guides readers to OIPC orders by section.[5]

There are more FIPPA case summaries on our website, where we regularly post new summaries.

## 3.1 FIPPA REQUESTS FOR REVIEW

### SECTION 3: SCOPE OF FIPPA

**Woman's Credit Rating Suffers after Wallet Stolen (Case Summary 1)**

Identity theft has reached pandemic proportions. Shredder sales have been very brisk in the last few years as people take whatever precautions they can to protect their personal financial information from dumpster-diving thieves. And if your wallet goes AWOL, you may need to report the loss of your cards without delay to avoid serious consequences.

A thief stole a woman's wallet and used her credit cards and other ID to obtain funds. To add insult to injury, the fraudulent use of her documentation damaged the woman's credit rating. To prove she had been victimized and re-establish her credit rating, she asked her municipal police department for copies of their records relating to the theft and subsequent fraud.

The police refused her request and told her the records were outside the scope of FIPPA. Section 3(1)(h) of FIPPA provides that the Act does not apply to records relating to a prosecution if all proceedings relating to the prosecution have not been completed. The woman asked our office to review the police force's decision.

Once we confirmed that the charges were still outstanding, it was clear that the position of the police department was correct. However, once we explained to the department the difficulties the woman was encountering as a result of the theft, they agreed to give her certain court documents that were public records. The police department also, with the agreement of Crown counsel, sent the woman a letter confirming the manner in which she had been victimized.

**Releasing Video Would Reveal Test Methodology (Case Summary 2)**

The parent of a child who had been given a psychological test asked the hospital that had conducted the test for a copy of the filmed assessment. The hospital replied that it was unable to grant access as the digital video recording was outside the scope of

[5] http://www.oipc.bc.ca/sector_public/orders_decisions/sectional_index.htm

FIPPA, being "a record of a question that is to be used on an examination or test" under section 3(1)(d).

The purpose of section 3(1)(d) is fairly self-evident – it protects information the disclosure of which might render a prepared examination ineffective. A psychologist at the hospital provided a detailed explanation of the reason why releasing the recording might be detrimental, noting that, as with all standardized psychological tests, the validity of the test depended on every test subject being equally naïve regarding the test content and materials. We considered this a convincing explanation of why section 3(1)(d) applied to the record in question.

### SECTION 13: POLICY ADVICE OR RECOMMENDATIONS

**Water District's Aquifer Study Not Exempt as Advice to a Public Body (Case Summary 3)**

A resident of a water district was concerned that new housing developments risked depleting the aquifer that supplied the community to the point that future water supplies might be jeopardized. Wanting to obtain more information to determine whether his concerns were justified, he asked the district for a copy of a hydrogeological study of the aquifer it had commissioned some time previously. When the district responded that it had decided to withhold the study under sections 13 and 17 of FIPPA, the resident asked us to intervene, as he felt that the contents of the study were a matter of public interest and the public had a right to know what it said.

On reviewing a copy of the study the district provided to us, we found it largely consisted of a detailed analysis of the structure of the aquifer. In addition, the study identified potential new well sites for accessing the underground water supplies.

Under section 13 of FIPPA, the head of a public body may refuse to disclose information that would reveal advice or recommendations developed by or for a public body. However, section 13 also provides that a public body must not refuse to disclose information such as factual material and feasibility or technical studies relating to projects of a public body. Under section 17, a public body may refuse access to information the disclosure of which could reasonably be expected to harm the financial or economic interests of a public body.

The district accepted our view that, insofar as the study was both technical and in large part factual, section 13 required the disclosure of the study, subject to any severing that might be reasonable under section 17. The district's primary concern, which lay behind its reluctance to release the study, was that publicly revealing the location of potential well sites might benefit competitors seeking access to the same water resources, to the detriment of the district. The risk of harm being both real and substantial, we concluded that the district's reliance on section 17 regarding this particular information was reasonable.

When we conveyed this conclusion to the resident, he told us he had no need to know the locations of potential well sites, so the district severed this information and gave him the balance of the study.

### SECTION 14: LEGAL ADVICE

**ICBC Severing Meets Litigation Privilege Test (Case Summary 4)**

A lawyer made an access request to the Insurance Corporation of British Columbia for the claim file of a client who had been involved in a motor vehicle accident. ICBC provided a copy of the file but withheld a considerable amount of information under sections 14, 17 and 22 of FIPPA.

ICBC maintained that it had appropriately applied the section 14 exception because the material in question consisted of communications between ICBC and its solicitors or records created in contemplation of litigation. Under the common law, a public body claiming litigation privilege must prove that the dominant purpose for creation of the record was to conduct, assist with or advise upon litigation under way or in reasonable prospect at the time of its creation. On reviewing the records, we were satisfied that this test had been met.

ICBC also made a persuasive case that the information it withheld under section 17 was information, such as reserve information (the estimated maximum cost of settling a claim), that, if disclosed, could harm ICBC's financial interests relating to the settlement of the claim. The information to which ICBC applied section 22 comprised the addresses, telephone numbers, insurance information, employment information and other information of third parties and was also justifiably withheld.

### SECTION 15: DISCLOSURE HARMFUL TO LAW ENFORCEMENT

**Why Accusers Deserve Privacy: The Case of the Barking Dogs (Case Summary 5)**

A couple in the BC interior who provided periodic dog-sitting and grooming services were surprised to receive a visit by their regional district's bylaw enforcement officer. The officer told them he was investigating a complaint that they were running a boarding kennel without a licence and that dogs were constantly barking on their property. Two days later, the officer sent them a letter notifying them that they had 30 days to close the operation. Later, following a second inspection, the bylaw enforcement officer became satisfied that the couple was not in fact boarding dogs overnight and withdrew the long arm of the law.

The couple demanded that the regional district send them all information in its possession about the complaint, including the name of the complainant, who was suspected of being a certain neighbour. The regional district wrote to them that it was unable to provide access to the records, under section 15(1)(c) of FIPPA, because disclosure might be harmful to the effectiveness of investigative techniques and procedures used or likely to be used in bylaw enforcement.

Past orders from our office have confirmed that, in order to withhold information under the discretionary section 15(1)(c) exception, a public body must be able to produce clear and cogent evidence, not mere speculation, of a rational connection between disclosure and the alleged harm. In this case, the regional district acknowledged to us that the harm it envisioned in withholding the records was speculative at best. Following discussion on this point, the regional district agreed to release to the couple the bylaw enforcement officer's notes about the kennel complaint, while blacking out the identity and contact information of the complainant.

Names of people complaining about legal infractions are sometimes withheld under section 15(1)(d), which authorizes the withholding of information the disclosure of which could reasonably be expected to reveal the identity of a confidential source of law enforcement information. They are sometimes also withheld under section 22(3)(b), which provides that disclosure of personal information is presumed to be an unreasonable invasion of privacy if it was compiled and is identifiable as part of an investigation into a possible violation of the law (except to the extent disclosure is necessary to prosecute the violation or continue the investigation).

**Reluctant Witness Brings Assault Trial to a Halt (Case Summary 6)**

The judge and jury had been selected and court dates had been scheduled for an assault trial when Crown counsel discovered that an important prosecution witness had decided not to co-operate. When a special prosecutor concluded that there was little chance of conviction without the testimony of the reluctant witness, the judge ordered a stay of proceedings.

The victim of the alleged assault, dissatisfied with the explanation for the stay of proceedings, sought access to Crown counsel's records on the case. The Criminal Justice Branch granted access to some records and withheld others under sections 14, 15 and 22 of FIPPA. Under section 15(1)(g), a public body may refuse access to information if disclosure could reasonably be expected to reveal information relating to or used in the exercise of prosecutorial discretion. Schedule 1 of FIPPA defines the "exercise of prosecutorial discretion" to include approving or not approving a prosecution, preparing for a trial, conducting a trial and staying a proceeding. The section 15(1)(g) exception to the general right of access to information is intended to permit candid discussions of the issues without fear that outside scrutiny will interfere with the decision-making process.

We reviewed the withheld records, which documented Crown counsel's approval of the charges, preparation for the trial and decision to stay the trial. The applicant accepted our view that section 15(1)(g) applied to all the withheld records and did not ask us to press forward on the applicability of sections 14 and 22.

**Ministry Cites Security Reasons for Withholding Security Audit (Case Summary 7)**

A reporter asked a ministry for a copy of a security threat and risk review report done by an internal audit unit of the ministry. The report dealt with potential security risks to a government-wide computer network.

The ministry withheld the report in its entirety, relying on the section 15 and 17 exceptions in FIPPA, especially on section 15(1)(l), which provides that the head of a public body may deny access to information the disclosure of which would "harm the security of any property or system, including a building, a vehicle, a computer system or a communications system". The reporter asked us to review the ministry's decision, emphasizing that he was simply seeking the auditors' evaluation of the state of security at the time of the review rather than details about the risks, and would be satisfied if only the report summary were released.

The ministry re-examined but did not alter its decision and told us that the decision had been made to withhold the report in its entirety because the information at issue

- identified likelihood, consequence and residual risk levels,
- could be used to compromise financial and business processes, resulting in financial loss or disruption of service, and
- pointed to areas of security vulnerability which, if released, could be used to attempt to exploit those vulnerabilities.

The ministry contended that releasing any information about the report could compromise the integrity of the security system controlling access to the government-wide computer network.

There has been relatively little interpretation of section 15(1)(l) in previous OIPC orders (see Order Nos. 60-1995 and 72-1995) and none dealing with circumstances such as those surrounding the auditor's report. We told the reporter of his right to request a formal inquiry, without speculating on the outcome. He decided to let the matter drop.

## SECTION 17: DISCLOSURE HARMFUL TO THE FINANCIAL OR ECONOMIC INTERESTS OF A PUBLIC BODY

**Release of Economic Model Could Harm Public Body's Negotiating Position (Case Summary 8)**

An applicant asked a public body for a copy of an "electronic model" that was used, during the development of a public sector infrastructure project, to make comparisons between the costs of a project utilizing the traditional "design/build" contracts and the costs of the same project utilizing "design/build/finance/operate" contracts, which are characteristic of a public private partnership (P3). The public body refused to disclose the electronic model, saying it fell under FIPPA's section 17 exception to the right of access to information.

After initially reviewing the file, we suggested to the applicant that the electronic model might fit the definition of a "computer program". A computer program is not a record, according to Schedule 1 of FIPPA, and would not be subject to FIPPA. The electronic model, while it could be accessed using a common software application, also contained additional proprietary applications created by a third party. Rather than simply being an electronic file that could be opened and viewed on a computer, the electronic model was described by the public body as an application that could receive input in the form of data and perform calculations to enable users to make financial comparisons.

Under section 17, a public body may refuse to release information the disclosure of which could reasonably be expected to harm the financial or economic interests of a public body. The public body argued that electronic models like the one the applicant requested also create benchmarks against which private sector P3 proposals are evaluated. The public body claimed that it was reasonable to expect that the disclosure of the electronic model could provide private sector P3 proponents with the ability to estimate more accurately the value of future projects and this could compromise a public body's evaluation process and cause harm by undermining the public body's negotiation position.

We concluded that the electronic model was likely not subject to FIPPA but, if it was, the public body's reliance on section 17 to withhold the model was reasonable. In an effort to resolve the dispute, the public body provided the applicant with a paper printout of the model. The applicant did not consider the printout satisfactory but did not pursue the review any further.

### SECTION 19: DISCLOSURE HARMFUL TO INDIVIDUAL OR PUBLIC SAFETY

**Rejected Arts Grant Applicant Demands Names of Jury (Case Summary 9)**

A Vancouver theatre group applied for a grant from the Spirit of BC Arts Fund, a BC government program intended to assist creative projects that contribute to the development of arts and culture in the province. After its application was rejected, the group wrote to the Ministry of Tourism, Sport and the Arts requesting a list of names of all the advisory committee members who adjudicated the application, all documents pertaining to the refusal of the application and all other documents written by administrators that might pertain to the application.

The ministry released all the requested records except for the names of the advisory board members, which it withheld under sections 19(1)(a) and 22(2)(e) of FIPPA, which authorize the withholding of information the disclosure of which could reasonably be expected to threaten anyone's health or safety. The ministry explained to us that an advisory committee member had once been assaulted at a cocktail party after participating in a decision to reject an application for funding. The applicant told

us that, without knowing who sat on the review committee, the theatre group had no way of knowing if advisory committee members had appropriate artistic backgrounds to qualify them to assess the group's application.

The cited sections of FIPPA have been the subject of orders that conclude that there must be evidence – which cannot be solely speculative – that the release of the records would threaten a third party's health or safety or cause a third party harm. After we brought this requirement to the attention of the ministry, it decided to release the list of names to the applicant. As a courtesy, the ministry contacted all of the affected advisory committee members and informed them of its decision. None of the members contacted expressed any concern about the release of their names.

### SECTION 21: DISCLOSURE HARMFUL TO BUSINESS INTERESTS OF A THIRD PARTY

**Bidder on Municipal Project Seeks Rivals' Bid Information (Case Summary 10)**

A bidder on a municipal project requested access to the bids put forward by other companies. The municipality released some of the information but withheld the unit pricing under section 21. The applicant asked our office to review the municipality's decision.

Section 21 of FIPPA requires public bodies to withhold information that would reveal a third party's commercial information under certain specific circumstances but also provides that this prohibition does not apply if the third party consents to the disclosure. During mediation, we requested that the municipality speak to the third parties about withholding their information. After examining the records at issue, the third parties agreed to the release of all the information.

### SECTION 22: DISCLOSURE HARMFUL TO PERSONAL PRIVACY

**Privacy in Public Spaces: Employer Withholds Surveillance Video Shot on City Street (Case Summary 11)**

After suffering an injury, a municipal worker took absences to recuperate. When the absences continued for a long period of time, the employer began to suspect the worker of malingering. Rumours that he was running a business on the side, selling items on city streets, simply heightened the suspicion. In preparation for possible disciplinary measures, the employer hired a private investigator to track and, in some cases, videotape the worker's movements.

The upshot was that the worker was eventually fired. As part of his efforts to grieve the dismissal, he filed a request for access to the videotape made by the private investigator. The municipality turned down the request, arguing that releasing the videotape would, under section 22 of FIPPA, be an unreasonable invasion of privacy of other people shown interacting with the worker on city streets.

Ordinarily, when a public body applies section 22 to materials requested under FIPPA, it will sever the personal information in question and release other parts of the

record to which FIPPA exemptions do not apply. In this case, however, the municipality argued that, because of the expense entailed in hiring a film editor's services, it could not reasonably sever the images of other people in the videotape and therefore had no obligation to do so under section 4(2) of FIPPA.

The request for access to the videotape thus raised two problematic questions: Did a lowered expectation of privacy in public places mean that releasing the videotape would constitute an unreasonable invasion of privacy of passers-by or of people seen conversing with the man under surveillance? And, if so, was it reasonable for the municipality to argue that the cost of blurring faces on the videotape meant it was entitled to withhold the videotape in its entirety?

Portfolio Officers in our office dealing with requests for review try to mediate resolutions that both comply with the law and are acceptable to the parties. In the event of an impasse, we will tell applicants of their right to request a formal inquiry resulting in a written order. Portfolio Officers may also, in providing this information, share with applicants their conclusions as to the likelihood of success at inquiry – there is little point encouraging requests for an inquiry where the issues are straightforward and have clearly been addressed in previous Commissioner's orders. The outcome in this case was by no means predictable, but the applicant decided not to request an inquiry.

**White-out Strikes Out as Severing Tool (Case Summary 12)**

A man in a battle with neighbours over property borders asked the regional district for copies of correspondence it had received from the neighbours. In due course, he received a package of records with a note that some information had been severed under section 22 of FIPPA because disclosing it would be an unreasonable invasion of the neighbours' personal privacy.

This he found puzzling because it wasn't obvious that anything had been deleted from the records. There were no lines or boxes or any other marks to indicate where the severed information had been. He complained to us that, because the regional district hadn't indicated what information was missing, he was not able to assess whether his right to obtain information had been respected.

The regional district explained to us that the only information it had deleted had been contact information (address, phone number, email address) of the neighbours, and, because white-out fluid had been used to make the deletions at the beginning or end of correspondence, naturally the deletions were not visible on photocopies. The regional district agreed to release another copy of the records, using pink highlighter to mark the parts of the page where the information was severed. After receiving the revised version, the complainant told us that he considered the matter resolved.

**Woman with Hereditary Disease Seeks Father's Medical History (Case Summary 13)**

A woman who had been adopted as an infant contracted a disease that she learned was frequently hereditary. Wanting to ensure that her children had the best health information available, she decided to try to find out the identity of her biological father. So she filed an access request for all records related to her adoption.

The ministry sent her a copy of the records but severed all information about her biological father, explaining that to divulge that information without his consent would have been an unreasonable invasion of his personal privacy under section 22 of FIPPA. The woman asked us to review the ministry's decision, emphasizing that she was only interested in finding out the ethnicity of her biological father (because her disease was far more prevalent in some racial groups than in others) and details of any health problems he might have experienced, rather than his precise identity.

Such requests have become more common because of increased understanding of links between genetic characteristics and incidence of certain diseases. As a result, the ministry has made arrangements with the Adoption Reunion Registry under which registry staff will review adoption records and disclose to adopted children information on their heredity without breaching confidentiality requirements. We told the woman about this option and she felt it was a reasonable compromise that might enable her to obtain the information she needed.

**Mother Requests Hospital Records to Find Out How Son Died (Case Summary 14)**

The mother of a young man who died in hospital wanted to find out the cause of death and how long her son had had to wait in Emergency for treatment. The health authority in charge of the hospital said it couldn't give her any information because her son had indicated his next-of-kin was his common-law wife, but she had moved right after the death and neither the hospital nor the mother had been able to contact her to see if she would consent to the hospital releasing information about how and why the man had died.

The health authority suggested the mother approach the Coroner Service for information, as an autopsy would probably have been done given that the son had died fewer than 24 hours after being admitted to hospital. However, the Coroner Service told her no autopsy had been performed. The mother then asked us to review the health authority's decision to deny her access to her son's information.

The health authority told us that they really wanted to help the mother obtain the information but felt their hands were tied by the *Freedom of Information and Protection of Privacy Regulation*, section 3 of which provides that the right to access or to consent to the release of information on behalf of a deceased individual may be exercised by the deceased's nearest relative or personal representative. As the deceased man had

named his common-law wife as his next-of-kin, the health authority felt it had no choice but to refuse his mother access to the records.

We brought the health authority's attention to section 22(2)(a) of the *Freedom of Information and Protection of Privacy Act*. It provides that, in determining whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the public body must consider whether the disclosure is desirable for the purpose of subjecting the activities of a public body to public scrutiny. Here, where the quality of treatment of the deceased man was one of the mother's primary concerns, it was reasonable for the health authority to consider the applicability of section 22(2)(a).

The health authority decided to release the information and the mother felt she had at last obtained closure to a painful episode in her life.

## 3.2 FIPPA ACCESS TO INFORMATION COMPLAINTS

### SECTION 4: INFORMATION RIGHTS

**Police Department Sets Tight Requirements for FIPPA Access (Case Summary 15)**

Concerned about a suspected fraud, the board of a housing co-op complained to the local police department. The police responded that they could only take a complaint from an individual, so the board appointed one of the directors of the co-op to file the complaint.

Following the conclusion of the police investigation, the office manager of the co-op wrote to the police department asking for a copy of the investigation report for the co-op's records. The police department denied the office manager access to the investigation report on the grounds that she wasn't a party to the original complaint. It suggested she obtain a copy from the co-op member who had originally made the complaint.

She found it puzzling that the board was unable to obtain information about an investigation that it had requested in the first place. After she complained to us, we reminded the police department that FIPPA makes no restrictions about who is allowed to exercise the right to gain access to non-personal information in the hands of public bodies. The police department then released the report to the applicant after severing certain information the disclosure of which would have resulted in an unreasonable invasion of the personal privacy of third parties.

### SECTION 5: HOW TO MAKE A REQUEST

**Journalist Objects to Demand for Access Request to Be Made In Person (Case Summary 16)**

In another instance, a reporter seeking access to police records was surprised to be told by the police department that, for his access request to be considered, he had to come

to the department's offices during business hours and fill out a form, even though the police department was several hours' drive from the reporter's home city. We drew the department's attention to section 5 of FIPPA, which requires only that an access request be made in writing – personal attendance is not required. The police department then called the reporter to let him know a mailed request would suffice.

### SECTION 6: DUTY TO ASSIST APPLICANTS

**Health Authority Goes Extra Mile Searching for Records (Case Summary 17)**

A health care worker asked his former employer, a health authority, for all records created within a specified time-frame and containing his personal information. He particularly wanted information that contained comments on the quality of his character or that related to his job applications within the health authority or his job performance. He named various types of records and a number of health authority employees he had communicated with as possible sources of records.

The health authority released what it could find but was unable to locate some records related to job applications and to correspondence the applicant claimed to have had with certain health authority employees.

As some information was severed from the records under section 22(1) of FIPPA and some of the records the applicant was expecting to receive were not included, he asked us to review the severing and also made a complaint that the health authority had not carried out an adequate search for records.

A review of the records found that only one line containing personal information had been severed. The document, a printout of the health authority's intranet site listing the names of job applicants who made online job applications, contained the personal information of the applicant and one other person. The severed information was the name and application status of the other person. Under section 22(1), the health authority was obliged to deny access to this information.

In support of his suggestion that the health authority had not carried out an adequate search, the applicant provided copies of records in his possession that he believed should have been produced.

The health authority agreed to carry out another search, particularly for the records the applicant provided to our office. It contacted 12 health authority employees, including those named by the applicant and employees who worked at the facilities named by the applicant, and the health authority's corporate office. These people were asked to search carefully for records related to the applicant and, if possible, suggest where records might be found. No additional records were found.

**Thorough Search by City Turns Up Everything but Emails (Case Summary 18)**

The applicant asked a city for all records relating to its approval of a covenant restricting the use of three multi-unit complexes to rental only for 10 years. The complexes

had been converted to condominiums and sold as individual units within the 10-year period to which the applicant believed the covenant applied. The city produced records in three phases from its legal department, its housing department and the city clerk's office. A search of the real estate department failed to produce any records. The applicant complained that the search was not adequate.

Section 6 of FIPPA requires a public body to conduct a search for records that a fair and rational person would expect to be done or consider acceptable. The search must be thorough and comprehensive. Evidence of the search should describe all potential sources of records, identify those searched and identify any sources not searched, with reasons for not doing so. The evidence should also indicate how the searches were done and how much time the public body staff spent searching for records.

In this case, the city provided a list of all departments searched, time spent in searching each department, a description of the standard records management practices of each department, a copy of the records classification system used by the city and an explanation of the mandate of each department. We concluded that the city's decision to search four departments was reasonable given the topic of the request and the mandate of the departments. We also concluded that the actual search of three of the departments was logical and thorough given the records management practices in the three departments.

A comparison of the records provided indicated that, although two individuals in particular appeared to have been actively involved in the covenant approval process, the records that were produced contained no emails from either of them. It became clear that the records management practices for the department in which the individuals worked had not been consistently followed. In general, emails were printed and filed, but the city reported that compliance was not universal. We concluded that the city should have searched the individual email accounts of the two individuals. As a result, the city undertook a further search and produced emails from one of the two individuals. The second individual no longer had email stored for the time period in question. We found the complaint to be partially substantiated.

**Lawyer Stymied in Hunt for Power Consumption Stats (Case Summary 19)**

A criminal lawyer who had occasional clients in the plant cultivation business concluded it might be a useful strategy to find out how much the amount of residential electrical consumption for residences varied over time. He asked the city to send him the monthly average electrical consumption for residential homes over a two-year period, as well as the yearly average.

The city responded by giving him year-by-year averages with per-house monthly consumption calculated by dividing the yearly total by 12 times the number of residential customers. It told him that it couldn't provide month-by-month averages through the

year because its hydro department only reads meters bi-monthly. Convinced that the city wasn't being straight with him, the lawyer sought our assistance.

The city explained to us that, although it didn't keep month-by-month statistics, its computer programmer could print off information that would provide month-by-month statistics based on the number of meters actually read in each month. While the result would not reveal the total power consumption of residential homes each month, it would enable the type of comparison the lawyer was seeking. The lawyer was happy with this solution and in due course obtained the statistics he needed without charge. The solution was consistent with the purpose of section 6(2)(b) of FIPPA, which provides that a public body must create a record for an applicant if it can be created from a machine-readable record using normal software and expertise and if doing so would not unreasonably interfere with its operations.

The city had correctly responded to the request as it had originally been worded by the lawyer. Our contribution was merely to look beyond the literal meaning of the original request and seek a means by which the city could meet the lawyer's need.

### SECTION 8: CONTENTS OF RESPONSE

**City Responds in Time, but Reasoning for Refusing Access Shaky (Case Summary 20)**

A man who emailed an access to information request to a city for internal correspondence complained that the city had not responded to his request in time, had not provided a reason for withholding one record and had not told him of his right to ask our office to review the city's response.

Section 7 of FIPPA requires a public body to respond to an access request within 30 business days. The complainant had not understood that "day" meant business day – the city had responded in time.

Section 8(1)(c)(i) requires a public body that refuses disclosure to give reasons for the refusal and the provision of FIPPA on which the refusal is based. In this case, the city had told the requester that it was withholding the record under section 12(1). When we pointed out that section 12(1) applies to Cabinet confidences at the provincial level rather than to local governments, the city realized its mistake and explained that it had intended to cite section 13(1), which applies to advice to a public body. As access to the record remained the complainant's ultimate objective, we opened a separate request-for-review file to address that matter and consider the city's section 13(1) argument.

The third part of the complaint related to the obligation of the city, under section 8(1)(c)(iii), to tell the requester of his right to request a review by our office of the city's decision to withhold information. The fact that his access request to the city had been by email and perceived to be of an informal nature made no difference to its validity, as the *Electronic Transactions Act* provides that a requirement for a document to be "in writing" includes electronic means. In addition, he had emphasized that "you

can consider this a written request via Freedom of Information and Privacy Act". He was thus correct that the city had had an obligation to advise him of his FIPPA right to ask us to review the city's decision, and we therefore found this part of his complaint to be substantiated. Fortunately, the complainant was fully aware of the role of our office. As many people are not, it is most important that public bodies ensure that their section 8(1)(c)(iii) obligation is met when they respond to a request.

SECTION 75: FEES

**Hard Line on Fee Waiver Request Softens during Mediation (Case Summary 21)**

A storm of controversy surrounded a proposal to develop a mine near a town. Because of the nature of the proposed operation, residents expressed grave concerns about the potential for air and water pollution in the surrounding area. A community group that strongly opposed the development made an access request to a provincial government ministry for all records related to the mine approval process.

In due course, the ministry replied that approximately 3,170 pages of records fell within the scope of the request and that it would process the access request on receipt of $1,585 to cover the cost of locating and retrieving the records, preparing them for disclosure and photocopying and mailing them.

Disappointed by the size of the proposed fee, the community group asked the ministry to consider waiving the fee, as the record related to a matter of public interest under section 75(5) of FIPPA.

The ministry responded that it was not in the habit of granting fee waivers and could see no reason to change its practice in this case.

The community group countered that its request appeared to satisfy the criteria that various OIPC orders had said public bodies should consider in determining whether a fee waiver was appropriate. First, the records related to a matter of public interest (the subject of the records had been a matter of recent public debate, the subject related to both the environment and public health and dissemination of the information could be expected to yield a public benefit). Second, the community group's primary purpose for making the request was to use or disseminate the information for public benefit. Third, the group was well placed to disseminate the information to the public through the internet and other means.

The ministry remained unmoved by these arguments.

The community group told us it had little in the way of funds and was in a poor position to be able to pay the requested fee. It asked us to review the ministry's decision not to waive the fee.

It appeared to us that the group had a fairly strong case to support its request for a fee waiver, but the ministry remained unconvinced and was not willing to negotiate.

We told the group it could either request a formal inquiry that might result in an order requiring the ministry to waive the fee or it could narrow the scope of its request to reduce the cost to a manageable level. The group decided to try reduce the scope of its request. Narrowing the time-frame and the type of records had the effect of reducing the fee estimate to $90.25 for 181 pages.

By this time, our office had managed to convince the ministry that all of the available evidence suggested that the group's request for a fee waiver met the tests and, as a result, the ministry decided to grant a fee waiver of $48.00, leaving the community group to pay only $42.25.

## 3.3 FIPPA PRIVACY COMPLAINTS

### SECTION 26: PURPOSE FOR WHICH PERSONAL INFORMATION MAY BE COLLECTED

**Privacy and Accuracy: Identifying Speakers at Public Meetings (Case Summary 22)**

A man who went to a public meeting organized by a municipality was surprised to see another citizen pick up the book listing speakers and begin writing down their names and addresses. He complained to the municipality about the apparent lack of security for people's personal information and found the response unsatisfactory.

The municipality told us its practice of asking all speakers at public hearings to put their names and addresses in the book was simply to ensure that the meeting secretary could accurately record them in the meeting minutes. As a result of our investigation, the municipality instituted a new policy of not collecting personal information for speakers' lists for public meetings. This satisfied the complainant and we closed the file.

### SECTION 30: PROTECTION OF PERSONAL INFORMATION

**A Privacy Breach in Every Double-stuffed Envelope (Case Summary 23)**

As a result of human error in the mail sorting room, a public body inadvertently double stuffed envelopes containing medical test results. The individuals receiving the envelopes received their own results and one other person's results. In total, 477 reports were inappropriately disclosed.

The OIPC immediately looked into the matter. With our assistance, the public body followed the four key steps we recommended for responding to privacy breaches (see our publication "Key Steps for Physicians in Responding to Privacy Breaches"[9]).

First, it took immediate mitigating steps by changing two key mail room processes and by contacting all individuals who had received other people's information in order to retrieve the medical test results.

As a second step, the public body assessed the risks associated with the breach and used that information to determine that notification was required and to identify longer-term strategies to reduce the chance of a recurrence of this type of error.

[9] http://www.oipc.bc.ca/pdfs/private/PhysicianKeyStepsPrivacyBreach.pdf

The third key step taken was to notify not only our office but also the individuals whose information was inappropriately disclosed and the doctors who had ordered the tests. The notifications said that the breach had occurred, described the steps taken to mitigate the problem and provided contact information for further assistance if needed.

Finally, the public body developed several new mail room processes and changes to the programming of the mail-sorting computer as a further safeguard against error.

SECTION 33: DISCLOSURE OF PERSONAL INFORMATION

**Job Applicant Objects to Personal Details on Driver's Abstract (Case Summary 24)**

An applicant for a job involving driving was asked to attach his driver's abstract with his resume. The driver's abstract provides a synopsis of a person's driving history. He later complained to us that the Insurance Corporation of British Columbia, in addition to describing a person's driving history in the driver's abstract, included unnecessary personal information such as age, sex and race, which a firm could conceivably use as an excuse not to hire someone.

We concluded that organizations should not require job applicants to submit their driver's abstracts until a commitment to hire subject to a clean driving record has been made. Our web resource for employers, "PIPA and the Hiring Process", emphasizes that employers must only collect personal information that is reasonably related to the hiring decision (for example, relevant formal qualifications, knowledge, skills and experience).

ICBC agreed with us that the complainant had expressed legitimate concerns about the mingling of detailed personal information with the driving history on the abstract. ICBC has included abstracts in an ongoing review of its policies on the disclosure of personal information.

## 3.4 FIPPA ORDERS

Those who are not satisfied with the outcome of mediation may request a formal inquiry, which involves an adjudication that results in a binding order. The summaries below reflect a selection of orders issued this year. All orders are published on our website.

**Insurance Council of British Columbia (Order F06-11)**

The applicant was the subject of a complaint to the Insurance Council of British Columbia by a former colleague (the "complainant"). In the course of responding to the Insurance Council's letter about the complaint, the applicant requested a copy of the "complaint letter outlining the allegations". In its response, the Insurance Council referred to the complainant by name and initially denied access to the complaint letters. During mediation of the applicant's request for review, the Insurance Council agreed to disclose the letters in severed form but denied access to third-party personal information and to some of the applicant's own personal information – in the form of other people's opinions about her – under sections 15(2)(b) and 22(1) of FIPPA.

In the inquiry, the Insurance Council acknowledged that, because of its complaint investigation, the applicant was aware of the complainant's identity and some of the complaint information. The Insurance Council argued that disclosing the remaining complaint information would unreasonably invade the complainant's personal privacy and could also reasonably be expected to expose the complainant to civil liability. The applicant disputed these arguments and said that a reasonable person should expect consequences from making defamatory remarks. She feared that the complaints would tarnish her reputation at work.

The Adjudicator concluded that section 15(2)(b) did not apply as section 243 of the *Financial Institutions Act* states that no action may be brought against someone as a consequence of making a communication to the Insurance Council in the course of investigations. The Adjudicator also found that section 22(1) did not apply to the applicant's personal information – that is, the complainant's comments and opinions about the applicant including identities of opinion holders.

**Provincial Health Services Authority (Order F06-15)**

The applicant requested access under FIPPA to a tape recording and a transcript of a meeting of a hospital committee respecting an infectious disease outbreak at the hospital that he had attended as a committee member. He was later dismissed from his position at the hospital. Various complaints, investigations and litigation ensued, including a defamation suit by the applicant against physicians and officials at the hospital, some of whom were also members of this committee who had attended the meeting in question. The applicant's defamation suit was dismissed at trial and he appealed it.

The Provincial Health Services Authority (PHSA) denied access to the tape and transcript, citing section 51 of the *Evidence Act*, a somewhat complex provision that prohibits disclosure of certain information or records regardless of most of the provisions of FIPPA. The applicant requested a review of this decision, alleging among other things that the PHSA had disclosed the tape to defendants in the defamation suit and to an investigator looking into some of the complaints.

After reviewing relevant case law on section 51 of the *Evidence Act*, the Adjudicator found that section 51(5) prohibited disclosure of the requested records and that, because of section 51(7) of the *Evidence Act* and section 79 of FIPPA, the prohibition on disclosure applied despite the applicant's right of access to records under FIPPA. The correctness or propriety of the disclosure and use of the tape and transcript in the other proceedings was not in the circumstances a matter for this FIPPA inquiry.

**Ministry of Environment (Order F06-16)**

The applicant, Sumas Energy 2 (SE2), and the provincial government participated in energy regulation hearings in the United States and Canada about an energy project SE2 had proposed. SE2 made an access request to the ministry for records about the

proposed energy project when the US hearings, but not the Canadian hearings, had concluded. The ministry issued a fee estimate of almost $9,000 and took time extensions under section 10 of FIPPA.

SE2 paid the fees and the ministry disclosed records in phases over a several month period, withholding information and records under sections 13(1), 14, 16 and 22 of FIPPA. SE2 requested a review of the ministry's decision to deny access under sections 13(1) and 14 and also complained that the ministry's disclosure of the records outside the legislated time limits frustrated the usefulness of the records to SE2 in upcoming Canadian Energy Board hearings. SE2 argued that, because of the delay, it should receive a refund of the fees it had paid, as a remedy under section 58(3)(c).

In the inquiry, the ministry argued that solicitor-client privilege applied to much of the information because (1) it was related to legal advice regarding the United States energy regulation hearings and was protected by legal professional privilege and (2) the energy hearings were litigation and much of the information had been prepared for use in the hearings and was thus protected by litigation privilege. SE2 rejected many of the ministry's arguments on solicitor-client privilege, saying for example that the energy regulation hearings were not litigation.

The Commissioner found that section 14 applied because legal professional privilege protected confidential communications regarding the hearings between the ministry and its lawyers and that litigation privilege also applied to much of the information. He also found that section 13(1) applied to some information. He found further that the ministry had not complied with the conditions of a time extension our office had granted the ministry under section 10(1)(c) and had failed to respond in time, effectively taking an unsanctioned time extension. He ordered a 50% refund of the fee as a remedy.

**Insurance Corporation of British Columbia (Order F06-18)**

The applicant made a claim to the Insurance Corporation of British Columbia for the loss by fire of his motorhome and its contents. While ICBC paid the applicant the payout value of the motorhome, it denied the claim for contents after some investigation. In response to the applicant's request for the claim file records, ICBC disclosed some information and records and denied access to others – principally investigation information – under sections 13, 14, 15, 16, 17, 19, 20 and 22 of FIPPA. Mediation of the applicant's request for review resulted in ICBC disclosing more information. ICBC also dropped sections 13, 16, 19 and 20 completely and, regarding some information, sections 14 and 17.

At the inquiry, ICBC claimed that both civil and criminal litigation were in reasonable prospect at the time of the creation of the records and that section 14 therefore applied. It also argued that disclosing the records could reasonably be expected to harm ICBC's future fraud investigations relating to fires and ICBC's financial interests as related to the litigation that ICBC claimed was in reasonable prospect. The Adjudicator found

that ICBC had not shown that litigation was in reasonable prospect and that section 14 therefore did not apply. The related claim that section 17 applied also failed. The Adjudicator also rejected ICBC's arguments regarding harm to its future fraud investigations and found that ICBC was not required to withhold a small amount of information under section 22.

**Village of Sayward (Order F07-05)**

The Village of Sayward denied the applicant access under section 14 of FIPPA to a legal opinion that the village's solicitors had provided in connection with a zoning issue about which local residents had expressed concern. After mediation of the applicant's request for review had failed, the village asked that the Commissioner exercise his discretion under section 56 not to hold an inquiry on the grounds that section 14 clearly authorized it to withhold the legal opinion. The Adjudicator denied the application as she believed there was an issue as to whether the village had waived privilege through certain actions in which it had referred to information in the legal opinion.

At the inquiry, the village argued that it had not waived privilege over the legal opinion through its actions, saying it had kept the opinion confidential and had not shown an intention to waive privilege. The applicant based much of his position on the reason for which the village obtained the opinion. The Adjudicator in the inquiry found that the village had not shown an intention to waive privilege in its conduct and that the partial disclosure had not caused unfairness and was not misleading. She found therefore that section 14 applied to the record.

**Elections British Columbia (Order F07-07)**

The Chief Electoral Officer dismissed the applicant from her appointment as a deputy district electoral officer, citing concerns about her performance of her duties. She then asked Elections BC for records related to her employment. Elections BC denied her request, saying that under section 3(1)(c), FIPPA did not apply to records related to the Chief Electoral Officer's functions under the *Election Act*. During mediation, Elections BC disclosed one of the records in severed form and provided a summary of the withheld information. It maintained its position that FIPPA did not apply to the records during mediation and at the resulting inquiry.

The Commissioner found that the records were captured by section 3(1)(c) of FIPPA as the Chief Electoral Officer had created them and they were in his custody and control and related to the exercise of his functions under section 18 of the *Election Act*. The Commissioner noted in passing that the applicant had already received the reasons for the termination of her appointment.

## 3.5 SUPREME COURT REVIEW OF OIPC's OPENNESS

As a public body under FIPPA, the OIPC must respond to access to information requests. Where an applicant is dissatisfied with the OIPC's response to a request, a BC Supreme Court judge acting as an adjudicator reviews our decision.

The OIPC has been the subject of a number of requests for review over the years. Several of these reviews have concerned our decisions to refuse access to requested records because they are excluded under section 3(1)(c) of FIPPA. This section states that certain records (which we refer to as our "operational" records) are excluded from FIPPA's scope. The adjudicators have confirmed the OIPC's decisions in such cases.

Only one such case arose this year. An individual objected to what he regarded as alterations to his "Statement of Claim" with the OIPC and alleged that the OIPC had failed to respond to his requests to correct personal information in our custody. Citing numerous previous adjudications on this topic, the OIPC made a preliminary objection to the individual's application on the grounds that, under section 3(1)(c), FIPPA does not apply to the records covered by the individual's alleged correction requests. Bauman J., acting as the adjudicator under section 62 of FIPPA, agreed and concluded that he had no jurisdiction to deal with the matter.

# 4 CASE SUMMARIES: PIPA MEDIATIONS AND INQUIRIES

The summaries below are grouped according to the sections of PIPA to which they most closely relate.

Further PIPA case summaries can also be found on our website, where we regularly post new summaries.

## 4.1 PIPA REQUESTS FOR REVIEW

### SECTION 23: ACCESS TO PERSONAL INFORMATION

**Persistence Pays Off in Patient's Quest for Medical Records (Case Summary 25)**

A woman wrote to her doctor requesting a copy of her medical files held in his office. Having received no reply four months later, she asked if we could help.

An organization's failure to respond to a request made under PIPA is termed a "deemed refusal", which we treat as a reviewable decision. In our file management processes, we give priority to deemed refusals and attempt to mediate a response as soon as possible.

The woman told us that, since her request, the physician had closed his practice and moved to the U.S. The doctor's office was closed and the phones were disconnected, but she understood that mail was being forwarded and that the receptionist had custody of the medical files. The complainant told us she now needed the records in order to find a new doctor in her community.

After mailing a complaint notification letter to the doctor's former address, we contacted the BC College of Physicians and Surgeons. The College told us it had no information about the location of the doctor's medical files, even though College guidelines advise physicians planning to move or close their practice to notify the College of the location of medical files and how they can be accessed. The doctor had, however, provided the College with his forwarding address in the U.S.

We sent a copy of our notification letter to the U.S. address but still received no response. We then made follow-up phone calls to the U.S. facility where the doctor was working, but our messages were not answered. Finally we wrote a letter to the doctor outlining the complaint, reminding him of his obligations to respond to information requests under PIPA and asking him to contact either the complainant or our office as soon as possible.

Soon after the letter was mailed, the doctor's wife, who also acted as his office manager, called to respond to our original notification letter. She told us that Canada Post was forwarding their office mail and she had just received our complaint notifi-

cation letter sent more than a month earlier. The doctor had not received any of the phone calls or letters sent to his U.S. address. When we described the complaint to the office manager she recalled the request by the complainant and also recalled that the complainant had been notified that the office was closing and that, if she wanted her records transferred to a new doctor, it would be done without charge but that she would have to pay a fee if she wanted the record copied for her personal use. According to the office manager, the complainant had not responded by the time the office was closed and it was assumed she had decided not pursue her request.

The office manager said they had notified both the College and all the doctors in their community about the location of their medical files and how they could be accessed. The College later acknowledged that it had received this information and should have made it available.

The office manager agreed to respond to the request from the doctor's U.S. location. This meant that the file would have to be sent to the office manager for screening and then back to the complainant. Since the most pressing issue was for the applicant to get a new doctor, we agreed to encourage the complainant to find a new doctor first, have the new doctor acquire her file and then make a request of her new doctor. The office manager wrote a letter to the complainant acknowledging her request and asked her to indicate whether she wished to continue with her request with her previous doctor or make the file request through a new doctor once she had found one.

The complainant decided on the latter course of action and said she considered her complaint resolved.

### Employer Ignores Former Worker's Request for Record of Hours Worked (Case Summary 26)

A former employee of a dental office made a request under section 23 of PIPA for copies of any records containing her personal information. After the dental office responded, she wrote back to say that she hadn't received a record of the hours she had worked each day. She asked for access to the ledger recording that information, emphasizing that she had no interest in obtaining the personal information of other staff. When the dental office denied the request, the woman asked our office to review that decision.

The dental office told us it had refused to release the information in the ledger because the woman already had all her payroll information on her payslips. However, it confirmed that the ledger contained the daily record of the hours worked by the applicant. We explained that, regardless of what the pay slips contained, the details of the hours worked were the former employee's personal information and should be released to her if the personal information of other staff could first be removed. The contact agreed to bring this up for discussion with the dentists at the office.

After agreeing to release a severed version of the ledger entries, the dental office sent it to us and asked us to send the record to the applicant. It is not our practice to

release records on behalf of public bodies or private sector organizations, so we asked the dental office to send the woman the record itself. We also noted that many of the severed ledger pages did not include the individual entry dates and the dental office contact agreed to make sure they were complete. In due course the applicant received the missing records and the matter was resolved.

**Sporting Body Gets Up to Speed on PIPA Responsibilities (Case Summary 27)**

A provincial sporting association investigated a complaint about the behaviour of one of its members and followed up with disciplinary action. When the member's lawyer wrote to the association requesting copies of records resulting from the disciplinary proceedings, the association acknowledged that the disciplinary proceedings were complete but did not respond to the request for records. The lawyer asked us to review the association's failure to respond.

When we contacted the association, it became apparent that its staff had vaguely heard of PIPA but were not familiar with its details or how the law applied to their organization. We explained how PIPA applies to the access request made on behalf of the affected individual. We explained that an organization must, within 30 business days, respond to a request by an applicant for access to his or her personal information. We also explained that, if access to all or part of the requested information is denied, the organization must tell the applicant why, with reference to the provisions of PIPA on which the refusal is based. We told the organization that PIPA also requires an organization to provide the name and contact information of someone in the organization who can answer questions about the refusal and to inform applicants that they have the right to request a review, within 30 days of being notified of the refusal, of the organization's response by the OIPC.

The association agreed to write another response letter that would fulfil its obligations under PIPA. The applicant's lawyer confirmed receiving the response letter and was satisfied with the association's response. No further action was required and our file was closed.

**Patient Doubts Doctor Took No Notes (Case Summary 28)**

A man complained to the College of Physicians and Surgeons that, when he showed up for an appointment with a urologist, the doctor refused to examine him. He also asked our office to review the urologist's refusal to give him a copy of his medical chart when he had requested it. He did not expect us to be successful in obtaining a medical chart from the doctor. Rather, he felt that the doctor's declaration to us that there was no chart would prove he had lied to the College when he told it he had examined the patient.

In response to the complainant's request for his personal information, the urologist had sent him a copy of the letter he had dictated to the referring specialist, describing

the visit and his examination of the patient. The urologist explained to us that, contrary to the complainant's belief, there were no other notes in the medical chart. The complainant had only visited him once and, as doctors pressed for time frequently do following patient visits, he had simply dictated a letter without taking notes.

**Fired Employee Not Entitled to Investigation Materials (Case Summary 29)**

A care-giver who worked in a seniors' residence got a call from the manager early one morning, as she was preparing to come to work, telling her she was suspended with pay pending the outcome of an investigation. When her employment was later terminated, she protested that she hadn't previously been informed of the allegations of abuse that were provided as the reason for the termination and had been provided no opportunity to defend herself.

A week later, she asked the company that ran the residence to release to her any information it had about her that related to the investigation and the reasons for her termination. The company replied that it was withholding this information under section 23(3)(c) of PIPA, which provides that an organization is not required to disclose an individual's personal information to the individual if the information was collected for the purposes of an investigation and the investigation and associated proceedings and appeals have not been completed.

In this case, the RCMP were still conducting a criminal investigation. Regardless of its merits or outcome, section 23(3)(c) clearly applied and the company was justified, for the time being, in withholding the information she had requested. We suggested that the applicant consult her lawyer about other possible legal avenues for obtaining the information she felt she needed to defend herself against what she maintained were unfair accusations.

## 4.2 PIPA COMPLAINTS

### SECTION 6: CONSENT REQUIRED FOR COLLECTION, USE OR DISCLOSURE

**Forged Consent Lands Broker in Hot Water (Case Summary 30)**

Organizations with access to databases of personal information must take care not to abuse the privilege. In this case, a mortgage broker, acting on the request of a client, agreed to submit a credit report request to Equifax, a company that maintains the credit histories and ratings of virtually all Canadians. The credit report was about a third party with whom the broker's client had had some business dealings. The third party did not know about the request nor did he consent to it.

All individuals in Canada are entitled to contact Equifax and request a copy of their credit report. Companies holding accounts with Equifax (such as banks, mortgage brokers, credit unions and retailers) request credit reports in order to determine whether

to extend credit or enter into certain business transactions with individuals. However, the company must have the consent of the individual whose credit report is being requested. In this case, the authorization signature of the person whose credit report was being sought had been forged. The third party found out about this unauthorized action and complained both to our office and to the Registrar of Mortgage Brokers at B.C.'s Financial Institutions Commission.

We began an investigation but deferred to the Registrar of Mortgage Brokers while the Registrar's staff conducted an investigation and a subsequent hearing that could have led to the imposition of penalties. Before the hearing, the mortgage broker admitted certain facts and entered into a consent order by which he was suspended for a period of time and agreed to pay the costs of the investigation.

PIPA provides a process by which a complaint may be investigated and a mediated resolution attempted. If not settled during that process, the complaint may on request proceed to an inquiry at which the Commissioner or Adjudicator may make a finding that a certain action was contrary to PIPA. Armed with the Commissioner's order, a complainant can then commence a court action for damages. In this case, the complainant was satisfied with the remedial measures imposed by the Registrar of Mortgage Brokers and chose not to pursue the PIPA matter any further.

### SECTION 7: PROVISION OF CONSENT

**Retailer Offers Rewards in Exchange for Personal Information (Case Summary 31)**

A regular customer of a national retail store was enticed by the promise of discounts and coupons to join its rewards program. Her enthusiasm soured, however, the day the store offered gifts to its rewards program customers but refused to give her one because she didn't have her membership card with her. She complained to us that the retailer was using personal information inappropriately and collecting unnecessary personal information as a requirement for providing a product, namely the free gift.

To become a member of the rewards program, customers have to provide their names and addresses. Once they have joined, the store also tracks their purchases. The complainant noted that the published purpose for collecting her personal information when she enrolled in the program was to provide customers with special offers, such as coupons, and other information. She contrasted that with a statement by an employee that customers' personal information was used to categorize the level of spending on an account and the shopping trends of the account user.

We decided that it was reasonable for the retailer to use a customer's shopping history to determine the kinds of special offers that would be most useful for each individual. We concluded that the retailer was not using the customer's personal information for a purpose other than the purpose stated on the application form. Any calculation of shopping trends was used by the retailer only to determine what offers

might be suitable or to determine what to stock in the store – a decision that would not affect individual members of the rewards program. The retailer also noted that its application form has an opt-out choice for customers who do not want special offers or the use of their personal information for this purpose. Customers who make this choice can still receive price discounts.

The woman also complained about the retailer's practice of providing gifts to rewards program members that are not available to other customers. She suggested that, since the collection of personal information from people joining the rewards program is not necessary in order to provide gifts, the retailer had violated section 7(2) of PIPA. This section states:

> *An organization must not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service.*

We disagreed with her conclusion. The purpose of section 7(2) is to prevent organizations from requiring customers to provide personal information that is not necessary for the transaction as a condition of being able to purchase goods or services. In the circumstances of this case, at least, customers who decide to withhold all personal information can still purchase goods in the retailers' stores. Nothing in PIPA prevents organizations from choosing to reward certain customers with gifts. Nor does PIPA require an organization to provide gifts to all customers simply because it singles out some for rewards.

In this case the retailer was not using the offer of a free gift to entice customers to provide unnecessary personal information. The retailer had already collected their personal information for the general purposes of the rewards program, namely to identify customers eligible for discounts and special offers. The gift was an added bonus for customers who had already joined the program.

## SECTION 11: LIMITATIONS ON COLLECTION OF PERSONAL INFORMATION

### Low-income Housing Collection of Tax Statements Complies with PIPA (Case Summary 32)

A resident in a seniors' housing complex asked us whether the housing society running the building had violated PIPA by requiring residents to verify their income by providing a copy of their Canada Revenue Agency tax statement (formally known as the Notice of Assessment). PIPA says an organization can only collect, use and disclose personal information if the purpose for collecting the personal information is reasonable in the circumstances and the personal information is necessary to provide the product or service.

Construction of the complex had been made possible in 1971 with the assistance of a loan provided to the original society members by the Canada Mortgage and

Housing Corporation. The terms of the loan allowed units to be leased only to low-income individuals or families who otherwise wouldn't be able to obtain suitable housing. The terms also required the society to obtain evidence of income from lessees and submit it to the CMHC at least once a year, the stated purpose being to ensure that the society was providing accommodation to low-income individuals or families. In this low-income housing complex, the rents were fixed at below-market rates and were related to the lessee's level of income. We concluded that the purpose for collecting income information was reasonable.

Was the collection of the personal information included in tax forms necessary to meet this purpose? In order to determine that new lessees meet the criteria for "low income", the society must collect evidence from the lessees about all their sources of income. One option for obtaining this evidence would be to collect from lessees all source documents providing evidence of income (such as statements from financial institutions). In our view, a less intrusive and more secure approach would be simply to collect a copy of a person's Notice of Assessment, which discloses net income for the year, from the Canada Revenue Agency. This would be simple, credible and subject to fewer security concerns. We concluded that the society's requirement complied with PIPA.

### SECTION 13: COLLECTION OF EMPLOYEE PERSONAL INFORMATION

**Job Applicant Objects to Collection of Excessive Information before Hiring (Case Summary 33)**

A man who applied for a position with a national retail chain objected to being asked to provide his social insurance number (SIN) on the company's job application form. While we were investigating this complaint, we also looked at the form's requirement that applicants provide information on criminal history and identify any relatives that were already working for the company.

The company explained that many applications come from people who are not eligible to work in Canada and it collects the SIN as a way of screening them out. It argued that collecting information about an applicant's criminal history is a reasonable occupational qualification given that employees have access to cash and merchandise. Finally, the company justified the collection of names of spouses or other family members already employed on the basis that company policy prohibits employees from being in a reporting relationship with a family member.

Under PIPA, businesses may only collect from job applicants information that is reasonably required to assess their suitability for a position. The SIN may only be collected after someone is hired because it is needed for income tax purposes. As a result of our investigation and mediation, the company agreed to change its job application form. In future, it will ask for only the first three digits of the SIN, thus providing the necessary information to the company without infringing on the applicant's right to keep that information confidential prior to hiring.

The company also agreed to restrict its requirement for information about criminal history by asking applicants to identify only whether they have been convicted of any of a list of particular criminal offences, such as theft or fraud, where that information is relevant to a fair assessment of their suitability for jobs with the company.

The company will also ask applicants only to identify any position held by a relative. This will enable the company to manage compliance with its policies without identifying particular individuals on the application form.

## SECTION 18: DISCLOSURE OF PERSONAL INFORMATION WITHOUT CONSENT

### "Pre-approved" Credit Card Mailing Draws Swift Response from Irate Consumer (Case Summary 34)

One day the mail brought an unexpected bonus: an unsolicited, pre-approved credit card issued by a Canadian bank with a $6,000 credit limit. The recipient, rather than being pleased by the invitation to spend, was sufficiently annoyed that he complained to the bank and demanded to know where it had obtained the personal information it needed to pre-approve and contact him.

The bank told him it had sent him the card because he held a private label credit card issued by an automotive supplies company and the bank's affiliate had recently taken over the contract to provide credit card services to the company. The complainant had applied for the private label credit card four years earlier in order to make a large purchase but had never used it again. The bank's representative assured him that its actions were completely legal.

The complainant then spoke to the automotive supplies company's credit manager, who gave him a somewhat different story. She said that, even though the bank's affiliate provided services for and maintained the company's private label credit card, it was in no way licensed or permitted to use the company's customer data base for direct solicitation or promotion of other bank products (such as credit cards).

Concerned that his personal information had been disclosed for purposes he had not consented to and that the new credit card might alter his credit rating, the man asked our office to investigate. Because federally regulated organizations are outside our jurisdiction, we referred his complaint about the bank's actions to the Privacy Commissioner of Canada. We also suggested that, with regard to his concern about his credit rating, he seek clarification from Equifax, one of the "big three" credit-reporting agencies operating in North America.

That left us with the issue of the automotive supplies company's disclosure of personal information to the bank. The company had hired the bank's affiliate to provide and administer the company's private-label credit card. The contract with the bank allowed it to access the company's customer information data bank but did not allow

the bank to share customer information for purposes other than providing the private label credit card services. The company's credit manager also told us that other customers had called to complain and that she had been frustrated by the bank's lack of response to the matter.

Before our investigation began, the company had already applied to the Supreme Court of British Columbia to prohibit the bank from using the company's customers' information to market credit cards. An out-of-court settlement was eventually reached between the company and the bank to halt the use of the company's customer information to market credit cards and the complainant considered the matter resolved.

SECTION 32: FEES

**Patient Seeks Access to Medical Records but Can't Locate Doctor (Case Summary 35)**

A man who wanted to obtain a copy of his medical records from his former doctor faced a significant hurdle: the doctor had retired and the man had no idea how to contact him. He wrote to the physician, care of the College of Physicians and Surgeons – the governing body for doctors in British Columbia – which in due course replied that the doctor had kept his records and would provide them for a fee. Section 32(2) of PIPA allows an organization to charge a minimal fee for access to an individual's personal information.

The man then complained to us that the College and the physician were not responding to him within a reasonable time. We contacted the College and the physician and arranged for the physician to provide the applicant with a fee estimate. The physician wanted to use the College as a go-between. The records were copied and provided to the College which, upon receipt of the fee from the complainant, released the records to him.

SECTION 34: PROTECTION OF PERSONAL INFORMATION

**Taking Files Home a PIPA Breach? Not If There's Adequate Security (Case Summary 36)**

An employee of an organization complained that the personnel manager had taken her personnel files home to work on them. The complainant believed that this contravened section 34 of PIPA as, in her opinion, the organization was not "making reasonable security arrangements" to protect her personal information.

Our investigation led us to conclude that, in this instance, taking the files home had not resulted in a breach of PIPA. The organization had informed its staff about their obligations to protect all information, including personal information. While the organization had not yet developed a written policy, as required by section 5 of PIPA, it had put in place a process for the removal of sensitive information from the office. This included sealing the information in a separate envelope and carrying files in a briefcase

that had to be kept in a locked car trunk while being transported. Once home, the files had to be placed in a locked filing cabinet in a locked office when not in use.

While we considered these steps to be reasonable security measures, we recommended that the organization spell out its procedures in a written policy and establish a process for auditing the use of personal information files outside the office to ensure those procedures were being followed. The organization agreed to do this.

**Law Files Blowing in the Wind (Case Summary 37)**

The confidentiality afforded a lawyer's client by way of the long-standing tradition of solicitor-client privilege means that law firms will routinely hold a great deal of personal information in their client files, be it matrimonial, tax, financial or medical information. For that reason, law firms must be especially vigilant in ensuring that records are properly and securely destroyed when no longer required.

Certain law firms in Victoria and Vancouver will remember 2006 as the year they tightened up their document-handling practices. A law firm in Victoria was the subject of a complaint to the OIPC by a concerned citizen who spotted client records with the firm's letterhead beside a dumpster near the firm's offices, and a Vancouver firm made the evening news in an unhappy fashion when similar client records were found blowing in the wind outside the firm's office building.

What we found in investigating each instance was that firms were trusting cleaning staff or building maintenance personnel to take records intended for secure destruction and recycling to recycling bins, where they would later be picked up. At one firm, cleaning staff inadvertently mixed client records with regular garbage and put them in a nearby dumpster. In the other case, records intended for secure shredding, for reasons unknown, never made it to a locked bin that was intended to provide a secure recycling service to the building's commercial tenants.

In each case, the system for secure destruction of client records was inadequate. The OIPC recommended and monitored the introduction of privacy-protective practices at each firm, which included having locked recycling bins reserved exclusively for sensitive records located in each firm's office rather than in a common building space or alleyway. These bins would then be emptied, and the client records securely shredded, by a contracted company specializing in secure document destruction. Cleaning staff or building maintenance personnel no longer played a role in the records management cycle. We considered the revised procedures adequate, but were left wondering how many other law firms might inadvertently be putting their clients at risk through inadequate document protection standards.

For that reason, we advised the Law Society of British Columbia (the governing body of the province's legal profession) about our concerns. The Law Society then sent a notice to its members reminding lawyers of the duty of client confidentiality set out in the *Professional Conduct Handbook* and of their privacy obligations under

PIPA. The notice provided a useful list of safeguards law firms should implement to protect client privacy.

**Client Files Vanish with Stolen Laptop (Case Summary 38)**

A lawyer had his laptop computer stolen from his desk while he was at lunch and the office receptionist was away from her desk. The laptop contained previous and current client files and information relating to legal work he had completed for his clients, including contracts, notarized documents, leases and wills.

The lawyer immediately notified the police and the Law Society of British Columbia, the governing body for lawyers. The police told him it was very unlikely that he would recover his laptop but that the thief would likely wipe the hard drive to eliminate any information that would identify the previous owner. The Law Society did not plan further action.

The lawyer used our office's recently developed Privacy Breach Reporting Form (posted on our website) to report to us the loss of his clients' personal information. As suggested on the form, the lawyer had conducted an assessment of the risk of the loss of personal information to his clients and to his firm. Client billing information was kept separate from client legal files and the laptop contained only names and addresses of clients and legal documents. There was no client financial information on the laptop.

We suggested that the lawyer notify his current and former clients of the loss of their personal information. He did so by letter for those for whom he had current addresses and contacted others directly by telephone. Fewer than 10 of his clients called him about the breach. Their concerns were alleviated when they learned that only limited personal information was on the computer.

To guard against similar breaches in the future, the law firm changed its policies to ensure that the receptionist was always at the front of the office during business hours and that the front door would be locked if she had to step away from the front desk. The firm also ensured that both laptop and desktop computers would be locked to desks to deter theft.

We were satisfied that the lawyer and his law firm had taken the necessary steps to

- contain the privacy breach and the risk of further breach;
- assess the risk to his clients of the loss of their personal information;
- notify his clients, and other relevant agencies, of the breach; and
- prevent future breaches of this nature.

## 4.3 PIPA ORDERS

Those who are not satisfied with the outcome of mediation may request a formal inquiry, which involves an adjudication that results in a binding order. The summaries below reflect a selection of orders issued this year. All orders are published on our website.

**An Incorporated Dentist's Practice (Order P06-01)**

The applicant requested access to her personal information in the hands of an organization, a dentist. The organization initially took the position that PIPA did not apply to records in its "College/Litigation" file, which consisted of records related to the applicant's complaint about the dentist to the College of Dental Surgeons. The organization said that it was therefore not obliged to respond to the request.

The organization later argued that the records did not contain the applicant's personal information but that, if they did, the organization was refusing access because the records contained the personal information of other individuals, information related to an investigation and information protected by solicitor-client privilege. It added that it could not sever the records. The organization also argued that the dentist was not an organization under PIPA and that PIPA did not apply to its "College/Litigation" file as the information in question had been collected before PIPA came into effect.

The Commissioner found that the dentist was indeed an organization under PIPA and that the records in dispute contained the personal information of the applicant and others. He also found that PIPA applied to the applicant's personal information in the organization's file and that she had a right of access to that information, subject to any exceptions.

The Commissioner found that the exception for third-party personal information did not apply to the applicant's own personal information in the organization's records but did apply to the personal information of the third parties. The Commissioner also accepted the organization's arguments that the requested personal information related to an investigation in that it pertained to the College's investigation of the applicant's complaint about the dentist. He said that he was satisfied that the organization was therefore authorized to withhold 15 of the 16 records. Because of this, the Commissioner said that the issue of severing the records did not arise. He added that, if he had not found that the organization was authorized to withhold the records under the exception related to investigations, he would have found it appropriate to sever the 15 records and disclose the applicant's personal information to her. The Commissioner was also satisfied that the sixteenth record was protected by solicitor-client privilege and that the organization was authorized to withhold it.

**Victory Square Law Office & British Columbia Nurses' Union (Order P06-02)**

The applicant submitted separate requests for his personal information to two organizations, which responded by saying that the information was subject to solicitor-client privilege and denied access under sections 23(3)(a), (c) and (e)(i) and 23(4)(a), (c) and (d) of PIPA. At the inquiry, the applicant argued that privilege did not apply, while the organizations argued that grievance arbitration proceedings are litigation for the purposes of solicitor-client privilege. The Commissioner agreed with the organizations and found that solicitor-client privilege applied to the requested records. He went on

to find that the requested records were protected by solicitor-client privilege and that the organizations could withhold them under section 23(3)(a) and 23(4).

**Langley CruiseShipCenters Ltd. (Order P06-05)**

The complainants, who were travel consultants, made a number of related allegations regarding unauthorized access, use and disclosure of their emails by the organization. At the inquiry, the Commissioner considered the issues of whether the information in question was personal information or employee personal information and whether the organization had complied with PIPA in collecting, using and disclosing that information. The complainants said, among other things, that the organization had gained unauthorized access to their email accounts and that it disclosed their emails to third parties. The organization said that it had concerns that the complainants were covertly using the organization's offices, equipment and confidential company information to set up rival businesses. It denied that it had disclosed any personal information except to a private investigator it had retained to investigate its concerns about the complainants and to the complainants themselves. As a result of this investigation, the organization terminated its relationships with the complainants.

The Commissioner found that the emails in question contained "personal information" about the complainants, as well as business "contact information". As this latter type of information is excluded from PIPA's definition of "personal information", the Commissioner concluded that PIPA did not apply to the organization's collection, use and disclosure of that information. He also found that the emails contained information on the complainants' business activities which he found was "work product information" and thus excluded from the definition of "personal information". The Commissioner also said that, even if the work product information were personal information, PIPA authorized the organization to collect, use and disclose it, without the complainants' consent, in order to investigate the organization's concerns about the complainants' activities.

**Twentieth Century Fox Film Corporation (Order P06-06)**

An individual who works in the film industry expressed concern about the organization's collection of information aimed at proving the applicant's residency in British Columbia during the year prior to filming for the purpose of obtaining tax credits. The complainant claimed that requiring this proof as a condition of employment violated mobility rights. The complainant also expressed concern about security arrangements for the information that the organization collected.

The Commissioner first considered whether the requested residency information was "employee personal information" and concluded that it was, as Fox requires the information in order to maintain its employment relationship with its employees. He then found that Fox's collection, use and disclosure of the residency information met PIPA's requirements.

## ORGANIZATION CHART

## FINANCIAL REPORTING

### 1. Authority

The Information and Privacy Commissioner is an independent officer of the Legislature who monitors and enforces compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). FIPPA applies to more than 2,200 public agencies and confers access to information and protection of privacy rights on citizens. PIPA regulates the collection, use, access disclosure and retention of personal information by more than 300,000 private sector organizations.

In addition, the Commissioner is the Registrar under the *Lobbyists Registration Act*, which requires those lobbying certain public agencies to register and pay a fee.

Funding for the operation of the Office of the Information and Privacy Commissioner (OIPC) is provided through a vote appropriation (Vote 5), as described below in note 3, and by recoveries for OIPC-run conferences. All OIPC payments are made from, and funds are deposited in, the Province's Consolidated Revenue Fund.

## 2. Significant Accounting Policies

These financial statements are prepared in accordance with generally accepted accounting principles in Canada. The significant accounting policies are as follows:

**a) Accrual basis**

The financial statements are accounted for on an accrual basis.

**b) Gross basis**

Revenue, including recoveries from government agencies, and expenses are recorded on a gross basis.

**c) Revenue**

Revenue is recognized when related costs are incurred.

**d) Expense**

Expense is recognized when goods and services are acquired or a liability is incurred.

**e) Net Assets**

The OIPC's net assets represent the accumulated cost of its capital assets less accumulated amortization.

**f) Statement of Cash Flows**

A statement of cash flows has not been prepared as it would provide no additional useful information.

**g) Capital Assets**

Capital assets are recorded at cost less accumulated amortization. Amortization is provided on a straight-line basis over the estimated useful life of capital assets as follows:

| | |
|---|---|
| Computer hardware and software | 3 years |
| Furniture and equipment | 5 years |

## 3. Appropriations

Appropriations for the OIPC are the subject of review and recommendations of the Legislative Assembly's Select Standing Committee on Finance and Government Services, as approved by the Legislative Assembly of British Columbia and included in the government's budget estimates as voted through the *Supply Act*. The OIPC receives approval to spend funds through separate operating and capital appropriations. Any unused appropriations cannot be used by the OIPC in subsequent fiscal years and are returned to the Consolidated Revenue Fund.

| | 2007 (UNAUDITED) | | | 2006 (UNAUDITED) |
|---|---|---|---|---|
| | OPERATING | CAPITAL | TOTAL | TOTAL |
| Appropriations | $2,539,000 | $30,000 | **$2,569,000** | **$2,241,000** |
| Gross Funds Available | $2,539,000 | $30,000 | **$2,569,000** | **$2,241,000** |
| Operating Expenses | -$2,314,703 | 0 | **-$2,314,703** | **-$2,157,267** |
| Capital Acquisitions | 0 | -$23,000 | **-$23,000** | **-$3,413** |
| **Unused Appropriations** | **$224,297** | **$7,000** | **$231,297** | **$80,320** |

### 4. Employee Benefits and Leave Liability

Accumulated liability with respect to vacation and other leave entitlements due to employees of the OIPC amounted to $12,983.24 as at March 31, 2007. This liability is fully funded in the Leave Liability Account.

### 5. Capital Assets

| | 2007 (UNAUDITED) | | | 2006 (UNAUDITED) |
|---|---|---|---|---|
| | COST | ACCUMULATED AMORTIZATION | NET BOOK VALUE | ACCUMULATED AMORTIZATION |
| Computer Hardware and Software | $89,984 | -$69,747 | $20,237 | $20,406 |
| Furniture and Equipment | $11,218 | -$3,706 | $7,510 | $0 |
| **Total** | **$101,202** | **-$73,456** | **$27,746** | **$20,406** |

### 6. Commitments

The OIPC has a leasehold commitment with ARES for building occupancy costs. Payments for office space for the fiscal 2007/08 are estimated at $149,193.00.

### 7. Pension and Retirement Benefits

The OIPC and its employees contribute to the Public Service Pension Plan in accordance with the *Public Sector Pension Plans Act*. The plan is a multi-employer defined benefit plan and is available to substantially all of the OIPC's employees. On behalf of employers, the British Columbia Pension Corporation administers the plan, including paying pension benefits to eligible employees.

The OIPC also contributes, through the Province's payroll system, for specific termination benefits as provided for under collective agreements and conditions of employment for employees excluded from union membership. The cost of these employee future benefits is recognized in the year the contribution is paid.